A Roadmap to Personal Data Protection & Privacy in Asia

November 2023

MERITAS®

A Roadmap to Personal Data Protection & Privacy in Asia

TABLE OF CONTENTS

Jeffrey Lim
Editor
jeffrey@joylaw.com
Director, Joyce A. Tan & Partners LLC

INTRODUCTION

Data protection and privacy laws around the world change constantly. And that's just the law.

New social, technological, or economic developments have data protection or privacy law implications every day.

Keeping up is essential.

When Meritas® last issued a guide, we covered the Asia Pacific, Europe, and USA in one book. Today, we'd need at least three.

And a big part of that is due to Asia.

Since that guide, China, India, Indonesia, Sri Lanka, and Thailand (who have 40% of the world population) each passed new laws, to say nothing of crucial updates in other countries.

And so, though we loved working with our Meritas® counterparts in Europe and America, this edition focuses on Asia, a complex region where each country rightly asserts its own sovereignty.

And digital sovereignty has become a key concern. Conducting business, with cross-border data transfers, is now a very nuanced affair.

We live in very interesting times.

To navigate these troubled waters, Meritas® has produced this guide, tapping on the minds of top-quality law firms in Asia to give an overview of each jurisdiction in a question-and-answer format, with contact details of practitioners who can help, if help is needed in this vital area of business.

ACKNOWLEDGEMENT

Special thanks go out to our Meritas® colleagues, including Yao Rao (China), my co-chair of the Meritas Asia Data Protection Practice Group, Eliza Tan (Meritas® Asia Regional Representative), Darcy Kishida (Japan), and all our contributors, whose hard work and support made this possible.

About Meritas

Meritas' global alliance of independent, market-leading law firms provides legal services to companies looking to effectively capture opportunities and solve issues anywhere in the world. Companies benefit from local knowledge, collective strength and new efficiencies when they work with Meritas law firms. The personal attention and care they experience is part of Meritas' industry-first commitment to the utmost in quality of service and putting client priorities above all else.

Founded in 1990, Meritas has member firms in 254 markets worldwide with nearly 9,000 dedicated, collaborative lawyers. To locate a Meritas resource for a specific need or in a certain market, visit http://www.meritas.org or call +1-612 339-8680.

MERITAS®

China

FIRM

AnJie Broad Law Firm
www.anjielaw.com

CONTACT

Samuel Yang
Beijing, China

Tel +86 10 8567 5988
yanghongquan@anjielaw.com

AnJie Broad is a full-service Chinese law firm with a wide range of practice areas. Its TMT team is a leading player in technology, data protection, and cybersecurity. AnJie Broad's practices in this area include personal information and data protection, cyber-security, AI, media, telecommunications, and internet services. Its clients include not only many well-known telecom operators and internet service providers at home and abroad, but also telecom and internet service users such as banks, insurers, automobile manufacturers, and pharmaceutical companies. This team is highly ranked by Chambers, Legal 500, LEGALBAND, and other professional legal research companies.

AnJie Broad's TMT team is led by Samuel Yang, former general counsel for BT in China. Samuel is a pioneer in data protection law in China and is one of a few lawyers with over 15 years of experience in data protection and cybersecurity matters. Chambers recognizes Samuel as a Band 1 lawyer in both "Data & Privacy" and "Technology & Telecoms."

China

FIRM

HHP Attorneys-At-Law
www.hhp.com.cn

CONTACT

Yao Rao
Shanghai, China

Tel +8621 50473330
yao.rao@hhp.com.cn

HHP Attorneys-At-Law is a leading law firm renowned for delivering exceptional professional solutions to clients worldwide. Adhering to the core value of "Quality First" and "Team Work," we are committed to achieving the best possible commercial and compliant outcomes for our diverse clients. HHP boasts a dedicated team offering comprehensive counseling and expert advice on cyber-security, data compliance, and relevant regulatory matters. Our extensive clients span various industries, encompassing Fortune 500 enterprises, transnational companies, large state-owned and privately-owned enterprises, as well as listed companies.

HHP's expertise in data compliance, corporate, M&A, and dispute resolution has been consistently and widely recommended by reputable guides like Chambers Global/Regional Guide, Legal 500, Thomson Reuters Asian Legal Business, Asialaw, IFLR 1000, and Benchmark Litigation, solidifying our reputation as a leading law firm in these practice areas.

Moreover, as an official member of the Information Security Management Working Group (WG7) of the National Information Security Standardization Technical Committee (TC260), we remain at the forefront of evolving regulations and best practices.

1. What are the major personal data protection laws or regulations in your jurisdiction? Is there any cross-sector legislation, and does it prevail over sector-specific legislation or vice versa?

In the People's Republic of China ("China"), personal data protection is primarily addressed by a set of rules centred around the term "personal information" ("PI"), including both cross-sector and sector-specific legislations.

The most important cross-sector legislation is the Personal Information Protection Law ("PIPL"), enacted in 2021, which sets forth comprehensive requirements for PI protection. Additionally, there are sector-specific regulations that provide more specific requirements in certain industries. A notable example is the Several Provisions on Automobile Data Security Management (for Trial Implementation), which provides detailed requirements for the protection of PI in the design, production, sales, use, and operation of automobiles. In China, sector-specific legislation is typically developed to further elaborate the provisions of the cross-sector legislation. In a case where sector-specific regulation provides more comprehensive requirements, the sector-specific regulation will prevail.

2. Which regulatory authorities are responsible for the implementation and enforcement of personal information protection laws?

In China, the enforcement of the PIPL is led by the Cyberspace Administration of China ("CAC") but may also include other regulators within their specific areas of competence, such as the Ministry of Industry and Information Technology (IT, telecoms, industry, etc.), State Administration for Market Regulation (consumers), the National Administration of Financial Regulation (banking, finance, insurance, etc.), the Ministry of Science and Technology (genetic), the Ministry of Public Security (crime), and many others.

3. How is "personal information"/"personal data" defined, and are there any categories of personal data that receive special or different protection (e.g., employees, minors, "sensitive" personal information, etc.)? If so, what are these categories, and can you summarize what special rules apply to these categories?

Under the PIPL, PI refers to any information, electrically or otherwise recorded, relating to an identified or identifiable natural person, excluding anonymized information. Sensitive PI means PI that, once leaked or illegally used, could easily lead to damage against an individual's dignity or pose risks to the individual's personal or property safety, such as biometric recognition information, religious beliefs, health information, financial accounts, whereabouts,

and any PI of minors under the age of 14.

Sensitive PI receives stricter protection, including:

(i) processing for a specific purpose with sufficient necessity and strict protective measures;

(ii) requiring separate notification to and consent from the individuals; and

(iii) conducting a prior PI protection impact assessment ("PIPIA").

Moreover, sector-specific regulations may impose more specialized requirements on PI in terms of automotive data, financial information, medical information, genetic information, and other specially regulated information.

4. What are the key principles under the major personal data protection laws or regulations relating to personal data?

Under the PIPL, the basic principles for processing PI include:

- lawfulness;
- legitimacy;
- necessity;
- good faith;
- openness; and
- transparency.

Other principles are mentioned or can be inferred. However, they can be considered derivatives of those listed above. The PIPL also explicitly states that PI processors may not act in any manner that is misleading, fraudulent, or coercive.

5. Are there any formal registration compliance requirements that apply to all businesses (e.g., the appointment of data protection officers, registration of databases, etc.)?

PIPL has not set universal registration requirements for all businesses. In certain cases, it may be necessary to file records with or report to competent authorities or carry out other administrative procedures. For example:

- PI Protection Officer ("PIPO"): if the volume of PI processed reaches a mandatory threshold, the processor should designate a PIPO and report his/her contact details to the competent authorities.
- Foreign Processor's Local Representative: for processors located outside Mainland China but processing PI of individuals in Mainland China for the purpose of providing products or services or analysing their behaviours, they should report to the competent authorities the contact details of their

appointed representative (either an institution or individual) in China to handle PI protection.

- Outbound Transfer of PI: please see Q7.

6. What obligations are there for organizations to establish compliance programs (e.g., legal and operational policies, contracts, etc.) relating to the processing, use, and disclosure of personal data?

Organizations in China are obligated to establish compliance programs relating to their processing activities. However, such obligations are high-level, meaning that PI processors have significant discretion regarding how they implement those obligations. Typical compliance programs cover things such as collection and use, notices and consent, contracted processing, disclosure and transfer, PI retention and deletion, PI subject rights, developing an internal management system and operating procedures, PI classification, access controls, training, technical and management security measures, impact assessments, security incident responses, cooperating with regulators, and, more generally, acting in accordance with Chinese laws and regulations.

7. What restrictions, if any, are there on personal data being transferred to other jurisdictions? How would organizations generally address these restrictions?

When providing PI of individuals within Mainland China to recipients outside Mainland China, the domestic provider should inform the individuals of the cross-border transfer in detail. The domestic provider should further obtain a separate consent from the individuals, conduct a PIPIA in advance, and retain records of the processing activities.

Moreover, depending on the circumstances of the domestic provider, as well as the nature and volume of the PI provided, different approaches would apply to transfer PI abroad.

If any of the following conditions are met, a security assessment for outbound data transfer by the CAC would be additionally required:

(i) the PI involves important data (as defined in the Data Security Law);

(ii) the provider is a critical information infrastructure operator;

(iii) the provider processes PI of more than 1,000,000 individuals; or

(iv) since January 1 of the previous year, the provider has provided PI of more than 100,000 individuals abroad, or the sensitive PI of more than 10,000 individuals abroad.

If none of the above conditions are satisfied, the provider may choose to lawfully transfer PI abroad by either signing a Standard Contract for Outbound Transfer of PI ("SCCs") and filing it (together with a PIPIA report) with the local cyberspace administration or by completing the PI protection certification. Based on our observations, unless the security assessment is mandatorily required, most domestic providers tend to prefer the option of the SCCs..

8. What restrictions, if any, are there on using or re-using personal data for data analytics/innovation or in adopting new business solutions such as artificial intelligence or data analytics? How would organizations generally address these restrictions?

When PI is used by PI processors for AI decision-making, transparency, fairness, and impartiality must be ensured, which, among other things, involves conducting an impact assessment. Unreasonable differential treatment in terms of transaction prices or other terms is prohibited. For AI decision-making used in business marketing or push-based information delivery, individuals must be given an option that does not target their personal characteristics or an easy way to stop receiving such communications. If an automated decision made by a PI processor significantly affects a PI subject's rights and interests, the PI subject may request an explanation and reject decisions made solely through automated means.

China has several regulations on algorithms and AI that require organizations to make filings or undergo security assessments of certain AI technologies, curate data used for training models, ensure the legality of AI outputs, and remediate problems with AI technologies within very limited timescales, e.g., the Administrative Provisions on Algorithm Recommendation for Internet Information Services.

As such, ensuring compliance with privacy laws throughout the whole lifecycle of any PI used to train AI should be a focus for organizations. Besides overcoming technical challenges for AI training, building up an internal compliance system through measures such as regularly conducting data analytics algorithm reviews and carrying out employee trainings on PI protection might be important.

9. What are the rights of an individual whose personal data is collected? Can they withdraw their consent, object to (and/or request deletion of) the retention of their personal data? If so, how?

The PIPL grants PI subjects the following rights: the right to be informed, the right to make decisions, the right to restrict or refuse processing, the right to withdraw consent, the right to access and copy, the right to data portability, the right to rectify or supplement, the right to deletion, and the right to request clarification of processing activities.

If processing is based on consent, PI subjects may withdraw their consent. In response, processors are required to provide convenient means for individuals to withdraw consent and to proactively delete the PI upon withdrawal.

In practice, PI subjects may exercise these rights through automated tools provided by the processor or through mechanisms publicly disclosed in the privacy policy or similar documents.

10. Are there any penalties, liabilities, or remedies if any of the personal information protection laws are violated?

Yes. Where processors violate the PIPL or fail to perform any PI protection obligations, the competent authorities could order a correction, confiscate any unlawful income, and issue a warning. If correction is not made, a fine of up to CNY 1 million may be imposed. For a serious law breach, competent authorities could impose a fine of up to CNY 50 million, or 5 percent of last year's annual revenue, and may also order the suspension of business and revoke the business permit.

Besides administrative penalties, the processor shall also bear the liabilities for damages to the PI subjects' rights and interests.

For serious offenses against PI, criminal liabilities might ensue.

11. Is there mandatory data breach reporting in your jurisdiction? If so, could you summarize the thresholds that trigger reporting, what should be reported and to whom, and what timelines are required/expected?

Under the PIPL, in the event of an actual or potential PI breach, alteration, or loss, the processor should promptly take remedial measures and notify the competent authorities, as well as the PI subjects. The above obligations to notify PI subjects may be exempted if the measures taken by the processor can effectively prevent harm caused thereby, but the competent authorities may still require the processor to perform the obligations.

12. Are there any recent notable developments in your country or cases that you think are likely to affect data privacy/data protection in the future? Is there anything else you would like to highlight?

2022 and 2023 witnessed the implementation of the three "legal paths" for cross-border transfer of PI under Article 38 of the PIPL, i.e., the security assessment, the SCCs, and the PI protection certification, as described in detail in Q7. The Measures for Cross-Border Data Transfer Security Assessments (2022), the Announcement on the Implementation of Personal Information Protection Certification (2022), and the Measures for Standard Contract for the Outbound Transfer of Personal Information (2023) constitute the Chinese legal framework for the PI cross-border transfer.

It is worth highlighting that Chinese regulators have recently taken significant steps towards establishing rules for artificial intelligence ("AI"). Specifically, China has released official guidance on how AI developers and service providers should ensure fair and non-discriminatory outcomes, including the Administrative Provisions on Algorithm Recommendation for Internet Information Services, the Administrative Provisions on Deep Synthesis in Internet-based Information Services, and the Interim Administrative Measures for Generative Artificial Intelligence Services. Furthermore, the Chinese government is taking focused measures to spur the development of AI technology, such as creating investment funds, offering tax relief to businesses involved in AI research and development, etc. As AI technology becomes increasingly incorporated into businesses, society, and people's personal lives, AI service providers in China need to pay close attention to the rapidly changing legal landscape in AI technology.

Hong Kong

FIRM

Gallant
www.gallantho.com

CONTACT

Philip Wong
Central, Hong Kong

Tel +852 2825 2607
philipwong@gallantho.com

Our firm was founded in 1977 and is a well-established and notable full-service independent firm in Hong Kong with over 40 solicitors. We offer comprehensive legal services to individuals and corporate clients, covering various aspects of legal services in corporate, commercial, and property related activities (contentious and non-contentious), including capital markets work, corporate and commercial, M&A, banking and finance, bond issuance, fund formation, China practice, trust and private clients, intellectual property, project developments and commercial real estate, conveyancing and tenancy, wills and probate, insurance, insolvency, mediation, arbitration, and litigation.

Hong Kong is the common law jurisdiction most preferred by both foreign and Mainland Chinese investors and enterprises for in-bound and outbound investments to and from Mainland China, in particular, using Hong Kong corporate vehicles as a base for fundraising and tax planning.

Our firm, with over four decades of experience in cross-border work, is in a privileged position to serve as a bridge for foreign investors and enterprises in Mainland China.

1. What are the major personal data protection laws or regulations in your jurisdiction? Is there any cross-sector legislation, and does it prevail over sector-specific legislation or vice versa?

The whole lifecycle of personal data from its collection to destruction is protected by the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong, enacted in 1995. The legislation obliges data users to comply with the six data protection principles and gives the data subjects a right to know what personal data is held about them.

The Ordinance was amended in 2012 to tighten regulation of corporate data users on the application of customers' personal data in direct marketing and sharing data with third parties. In 2021, the Ordinance underwent further major amendments to combat doxxing acts that are intrusive to personal data privacy. The Commissioner is also empowered to conduct criminal investigation, institute prosecution for doxxing cases, and serve cessation notices to demand the removal of doxxing contents.

The primary and prevailing personal data protection legislation in Hong Kong is the Personal Data (Privacy) Ordinance which applies to all sectors, and it shall prevail over any other sector-specific legislations. The Commissioner also issued various codes of practice which are non-binding, but any breach will give rise to a presumption against a data user in any legal proceedings under the Ordinance.

2. Which regulatory authorities are responsible for the implementation and enforcement of personal information protection laws?

The Privacy Commissioner for Personal Data is an independent statutory body set up to oversee and enforce the implementation of the legislation. Members of the public who wish to make an inquiry or lodge a complaint to the Commissioner should proceed to its office, currently at Unit 1303, 13th Floor, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong or reach them by email at communications@pcpd.org.hk. Further details can be found on its website at https://www.pcpd.org.hk.

3. How is "personal information"/"personal data" defined, and are there any categories of personal data that receive special or different protection (e.g., employees, minors, "sensitive" personal information, etc.)? If so, what are these categories, and can you summarize what special rules apply to these categories?

Under the Ordinance, "data" means "any representation of information (including an expression of opinion) in any document and includes a 'personal identifier'."

"Personal data" means "any data—

(a) relating directly or indirectly to a living individual;

(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and

(c) in a form in which access to or processing of the data is practicable."

"Personal identifier" means "an identifier that is assigned to an individual by a data user for the purpose of the operations of the user; and that uniquely identifies that individual in relation to the data user, but does not include an individual's name used to identify that individual."

The definitions are limited to the personal data of individuals. Information identifying legal entities such as corporations and companies is not included in the definition, but information identifying individual partners of a partnership is included.

No specific categories of personal data are expressly reserved for stronger protection in the Ordinance. However, the Commissioner has issued codes of practice setting out specific requirements in respect of certain kinds of personal data, such as human resource management and monitoring and personal data privacy at work. The Commissioner also recommended warning messages may be adopted in online form to alert children of the minimum amount of information to supply and to remind young children to consult parents or teachers when providing their personal data online.

4. What are the key principles under the major personal data protection laws or regulations relating to personal data?

Data users are required to comply with six data protection principles ("DPP").

DPP 1 - Personal data must be collected in a lawful and fair way for a legitimate purpose directly related to a function or activity of the data user. Data subjects must be notified of the purpose and the classes of persons to whom the data may be transferred and whether it is obligatory to supply the data and, if so, the consequences of refusal. The data collected should be necessary but not excessive.

DPP 2 - Personal data must be accurate and must not be kept for longer than necessary to fulfill the purpose for which it is collected and used.

DPP 3- Personal data must be used for the specified purpose or a purpose directly related to it, unless voluntary and explicit consent with a new purpose is obtained from the data subject.

DPP 4- There must be measures against unauthorized or unlawful access, processing, erasure, loss, or use of personal data.

DPP 5 - There must be measures to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.

DPP 6 - Data subjects must be given access to their personal data and allowed to make corrections.

5. Are there any formal registration compliance requirements that apply to all businesses (e.g., the appointment of data protection officers, registration of databases, etc.)?

There is currently no statutory requirement to register databases regarding the collection or use of personal data. There is also no statutory requirement to appoint a data protection officer and no penalty for not doing so.

6. What obligations are there for organizations to establish compliance programs (e.g., legal and operational policies, contracts, etc.) relating to the processing, use, and disclosure of personal data?

There is no statutory requirement for organizations to establish compliance programs. However, the Commissioner encouraged organizations to develop their own privacy management programs and appoint a data protection officer to oversee the organization's compliance of the Ordinance.

7. What restrictions, if any, are there on personal data being transferred to other jurisdictions? How would organizations generally address these restrictions?

While there are currently no restrictions on transfer of personal data outside Hong Kong, the Commissioner issued a Guidance Note on Personal Data Protection in Cross-border Data Transfer supplemented by a Guidance on Recommended Model Contractual Clauses for Cross-border Transfers of Personal Data and provided two sets of Recommended Model Contractual Clauses to cater to two different scenarios in cross-border data transfers, namely, (i) from one data user to another data user; and (ii) from one data user to a data processor to facilitate the parties to cross-border transfers of personal data to take into account the relevant requirements of the Ordinance.

However, organizations are still required to comply with the general requirements of the Ordinance to ensure that the transfer of personal data outside Hong Kong must be for the purpose for which the data was to be used at the time of the collection of the data or a directly related purpose.

8. What restrictions, if any, are there on using or re-using personal data for data analytics/innovation or in adopting new business solutions such as artificial intelligence or data analytics? How would organizations generally address these restrictions?

Organizations may only use the personal data for the purposes disclosed to the data subject on collection or a directly related purpose unless the use falls within the exemptions set out in the Ordinance, such as, (1) the data is to be used for preparing statistics which are not to be used for any other purpose, and (2) that the resulting statistics are not made available in a form which identifies the data subjects. Any usage of personal data for new purposes requires the prescribed consent of the data subject. Organizations should take steps to ensure that the data is collected for a lawful purpose directly related to a function or activity of the data user, the collection is necessary for or directly related to that purpose, the data to be collected is not excessive, and practical steps are taken to ensure that the data subject has been informed, on or before collection of the data, of the purpose for which the data will be used and that the data should not be kept longer than necessary.

9. What are the rights of an individual whose personal data is collected? Can they withdraw their consent, object to (and/or request deletion of) the retention of their personal data? If so, how?

Individuals have the right to:

(i) make a data access request and know the reason for the refusal of such request;

(ii) request the correction of incorrect data and know the reason for the refusal of such request;

(iii) request the erasure of incorrect data;

(iv) require that their personal data is not used for direct marketing;

(v) make a complaint to the Commissioner about contravention of the legislation;

(vi) claim compensation in civil proceedings where they have suffered damage as a result of a data user's failure to comply with the legislation and may ask the Commissioner for assistance in the proceedings; and

(vii) withdraw their consent to the retention of their personal information by a third party by informing the data user (i.e., the person who collected their data) of their withdrawal.

10. Are there any penalties, liabilities, or remedies if any of the personal information protection laws are violated?

The Commissioner can issue enforcement notices directing a person in breach of any data protection principle to take steps to remedy and prevent any recurrence of the contravention. Contravention of an enforcement notice or intentionally doing the same act or making the same omission specified in the enforcement notice may result in a fine and imprisonment. Disclosing any personal data obtained from individuals without their consent with the intention of obtaining gain in the form of money or other property or to cause loss to them is an offense. Any such disclosure causing psychological harm to them is also an offense. A person in breach of the legislation may also be faced with a civil claim.

The Commissioner can carry out criminal investigations for doxxing cases, institute prosecution, and demand the cessation of doxxing contents.

11. Is there mandatory data breach reporting in your jurisdiction? If so, could you summarize the thresholds that trigger reporting, what should be reported and to whom, and what timelines are required/expected?

There is currently no legal requirement to report a data breach. However, the Commissioner issued a non-binding guidance note encouraging data users to notify the affected data subjects, the Commissioner, the relevant law enforcement agencies and regulators, and such other parties who may be able to take remedial actions to protect the personal data privacy and interests of the data subjects affected. That said, data users may be liable under the Ordinance for failing to apply appropriate security measures to personal data.

12. Are there any recent notable developments in your country or cases that you think are likely to affect data privacy/data protection in the future? Is there anything else you would like to highlight?

The Commissioner, in a briefing to the Legislative Council on February 20, 2023, announced that substantive amendments to the Ordinance will take place, which include:

(i) establishing a mandatory data breach notification mechanism;

(ii) introducing direct regulation of data processors;

(iii) requiring formulation of a data retention policy; and

(iv) empowering the Commissioner to impose administrative fines.

These proposed amendments would bring material reform to the Ordinance and strengthen the protection of personal data privacy in Hong Kong.

CONCLUSION

Data users should familiarize themselves with the Personal Data (Privacy) Ordinance, the six data protection principles, codes of practice, guidelines, and guidance notes. Codes of practice are not legally binding, but any breach will give rise to a presumption against a data user in any legal proceedings under the Ordinance. Guidelines and guidance notes indicate the manner in which the Commissioner proposes to perform its functions or exercise its powers under the law. They represent the best practices in the opinion of the Commissioner, but any breach will not necessarily give rise to legal liability.

India

FIRM

Khaitan & Co LLP
www.khaitanco.com

CONTACT

Harsh Walia
Mumbai, India

Tel +91 11 4151 5454
walia@khaitanco.com

Khaitan & Co was founded in 1911 and is among India's oldest and most prestigious full-service law firms. It is also one of the largest, with 1000+ professionals and 230+ partners, counsels, and directors. The firm's teams, comprising a powerful mix of experienced senior lawyers and dynamic rising stars in Indian law, offer customized and pragmatic solutions that are best suited to their clients' specific requirements. The firm acts as a trusted advisor to leading business houses, multinational corporations, financial institutions, governments, and international law firms. From mergers and acquisitions to intellectual property, banking to taxation, capital markets to dispute resolution, and emerging areas like white-collar crime, data privacy, and competition law, the firm has strong capabilities and deep industry knowledge across practices. With offices in New Delhi, Noida, Mumbai, Bengaluru, Chennai, and Kolkata, the firm also has capabilities in overseas markets via its country-specific desks and robust working relationships with top international law firms across jurisdictions. The firm opened its first international office in Singapore in 2021.

1. What are the major personal data protection laws or regulations in your jurisdiction? Is there any cross-sector legislation, and does it prevail over sector-specific legislation or vice versa?

Presently, India does not have comprehensive data protection legislation. Such provisions are encapsulated in the Information Technology Act 2000 ("IT Act") and rules framed under it ("SPDI Rules") alongside sector-specific legislations that coexist and complement the IT Act.

Generally, sector-specific laws take precedence over broader general laws. However, they may be limited. Hence, the IT Act fills the gaps and ensures comprehensive data protection.

On August 11, 2023, the Digital Personal Data Protection Act, 2023 ("DPDP Act") was enacted. It will replace the framework under the IT Act and SPDI Rules once it formally comes into effect and prevails when in conflict with other data protection legislation.

2. Which regulatory authorities are responsible for the implementation and enforcement of personal information protection laws?

While there is currently no such overarching regulatory authority, the DPDP Act envisages the constitution of a Data Protection Board for such purposes.

3. How is "personal information"/"personal data" defined, and are there any categories of personal data that receive special or different protection (e.g., employees, minors, "sensitive" personal information, etc.)? If so, what are these categories, and can you summarize what special rules apply to these categories?

According to SPDI Rules, "personal information" ("PI") is any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available to a body corporate, is capable of identifying a person.

The SPDI Rules predominantly affords protection to "sensitive personal data or information" ("SPDI"), defined as PI relating to:

(i) password;

(ii) financial information such as bank account, credit card, debit card, or other payment instrument details;

(iii) physical, physiological, and mental health conditions;

(iv) sexual orientation;

(v) medical records and history;

(vi) biometric information; etc.

Information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other laws is excluded from the purview of SPDI.

Once effective, the DPDP Act will afford protection to all "personal data" in a digital form, except personal data processed by an individual for any personal or domestic purpose and personal data that is made or caused to be made publicly available.

4. What are the key principles under the major personal data protection laws or regulations relating to personal data?

While the IT Act and the SPDI Rules do not expressly set out key principles for data protection, the following may be noted:

(a) Consent is the only lawful basis for collection of PI: Written consent (including by way of electronic means) is the only grounds for collection of SPDI.

(b) Transparency: Entities collecting SPDI must ensure that the provider of SPDI knows (i) that information is collected, (ii) the purpose for collection, (iii) the intended recipients of the information, and (iv) the name and address of the agency that is collecting the information and that the agency will retain such information.

(c) Purpose limitation: SPDI should not be collected unless for a lawful purpose connected with the function of the entity.

(d) Data minimization: SPDI should not be collected unless such collection is considered necessary for that purpose.

(e) Storage limitation: Entities holding the SPDI should not retain it for longer than is required for the purposes for which the information may lawfully be used or otherwise required under any other law.

The DPDP Act is also based on other principles such as usage of personal data in a lawful manner, using data only for the purpose it was collected for, accuracy of personal data, implementation of reasonable safeguards, and accountability of data fiduciaries.

5. Are there any formal registration compliance requirements that apply to all businesses (e.g., the appointment of data protection officers, registration of databases, etc.)?

There are no specific registration compliance requirements currently. However, general obligations for entities collecting or processing SPDI include designating a grievance officer and publishing their contact details, implementing reasonable security practices and procedures ("RSPP"), and conducting periodic audits. The DPDP Act also envisages the appointment of a Data Protection Officer and independent auditor for "significant data fiduciaries" (which are yet to be classified).

6. What obligations are there for organizations to establish compliance programs (e.g., legal and operational policies, contracts, etc.) relating to the processing, use, and disclosure of personal data?

Entities collecting and processing SPDI must provide a privacy policy to the data subjects and ensure that it is "available for view." The SPDI Rules prescribes that the privacy policy should be published on the entity's website and inform the provider of:

(a) information regarding type of personal information and SPDI collected;

(b) its practices and policies;

(c) any disclosure to third parties; and

(d) RSPP adopted by the entity.

For RSPP, the SPDI Rules recognize the international standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements" for implementation. Under the SPDI Rules, a comprehensive and documented information security program and policies containing managerial, technical, operational, and physical security control measures that are commensurate with the information assets being protected, must be prepared and implemented. These measures should be audited through an independent auditor at least once a year or when the entity undertakes significant upgradation of its process and infrastructure.

In comparison, the DPDP Act sets out more robust obligations for organizations depending on the role it undertakes. However, many aspects are yet to crystallize and the Government is expected to issue further rules/notification.

7. What restrictions, if any, are there on personal data being transferred to other jurisdictions? How would organizations generally address these restrictions?

Under the SPDI Rules, disclosure and transfer (including cross-border transfer) of SPDI is permitted where:

(a) SPDI is collected under a lawful contract and the provider of SPDI has given permission for disclosure to any third party; or

(b) disclosure is necessary for compliance with a legal obligation.

Third parties to whom SPDI is disclosed must not disclose it further.

Additionally, transfer (including cross-border transfer) of SPDI is allowed where:

(a) necessary for performance of a lawful contract between the entity and provider of SPDI or where the provider of SPDI has consented to such transfer; and

(b) the transferee/recipient entity ensures the same level of data protection as prescribed under SPDI Rules.

For the avoidance of doubt, there are no blanket restrictions under the IT Act, but certain sectoral laws may have data localization requirements.

Practically speaking, organizations should ensure that prior permission of the user is obtained for sharing their SPDI and suitable protective measures are undertaken before disclosure/transfer. Organizations may also contractually ensure that any entities/persons to whom any information is transferred afford the same level of data protection as prescribed under the SPDI Rules.

The DPDP Act currently permits processing of personal data outside India (unless restricted by the Government by notification), subject to general obligations under the DPDP Act.

8. What restrictions, if any, are there on using or re-using personal data for data analytics/innovation or in adopting new business solutions such as artificial intelligence or data analytics? How would organizations generally address these restrictions?

There are no specific restrictions on re-using personal data for data analytics or other similar purposes. However, the SPDI Rules require that SPDI be collected for a lawful purpose connected with the function or activity of the company, and collection is necessary for that purpose. Further, entities collecting SPDI are required to inform the provider of SPDI about the purpose for collection. The DPDP Act also sets out similar principles for the processing of personal data.

Hence, organizations intending to re-use personal data should inform the providers of information about the different purposes the data may be used for and seek appropriate consent.

9. What are the rights of an individual whose personal data is collected? Can they withdraw their consent, object to (and/or request deletion of) the retention of their personal data? If so, how?

The SPDI Rules sets out the rights of providers of SPDI. Notably, any entity collecting/processing SPDI (or other entities on its behalf) is required to inter alia provide an option to the provider of the information to:

(a) not provide the information sought to be collected; and

(b) withdraw consent (in writing) given previously.

Per the SPDI Rules, providers of information, upon request, must be permitted to review the information they provided, and personal information or SPDI found to be inaccurate or deficient shall be corrected or amended as feasible.

Although the SPDI Rules do not prescribe formal mechanisms for providers of SPDI to exercise their rights, they may typically be exercised by writing to the grievance officer designated by the entity.

While the SPDI Rules do not expressly envisage the right to erasure/right to be forgotten, the High Courts of various states in India have adopted contradicting views on the same. Several have recognized the right to be forgotten as a part of right to privacy of an individual, but some have also refused to enforce this right except in certain cases. Hence, the position on right to erasure/right to be forgotten remains unsettled.

Separately, the DPDP Act sets out extensive rights for data principals, including right to access information about personal data, right to correction and erasure of personal data, right to grievance redressal, and right to nominate. Where consent is the basis for processing of personal data, the data principals have the right to withdraw their consent at any time.

10. Are there any penalties, liabilities, or remedies if any of the personal information protection laws are violated?

Per the IT Act, an entity possessing, dealing, or handling any SPDI, who is negligent in implementing and maintaining RSPP and, as a result, causes wrongful loss or wrongful gain to any person will be liable to pay damages by way of compensation to the affected person.

Further, the IT Act prescribes imprisonment and imposition of fines for unauthorized disclosure of personal information with the intent to cause or knowing that it is likely to cause wrongful loss or wrongful gain.

However, the on-ground enforcement of these provisions has been rather bleak.

In contrast, the DPDP Act sets out hefty penalties depending on the nature of breach/non-compliance, and a more comprehensive dispute resolution and enforcement mechanism.

11. Is there mandatory data breach reporting in your jurisdiction? If so, could you summarize the thresholds that trigger reporting, what should be reported and to whom, and what timelines are required/expected?

The IT Act and SPDI Rules do not set out data breach reporting requirements.

However, there are such requirements under directions issued by the Indian Computer Emergency Response Team, pursuant to the IT Act. All entities are required to mandatorily report certain types of cyber incidents and cyber security incidents to Indian Computer Emergency Response Team within six hours of noticing such incident or being notified about such incident, in the prescribed manner. Additionally, there are breach reporting requirements under sectoral laws such as finance and insurance which prescribe different timelines and thresholds for breach reporting.

Further, under the DPDP Act, any "personal data breach" needs to be intimated to the Data Protection Board and each affected data principal in the manner as may be prescribed by the Government.

12. Are there any recent notable developments in your country or cases that you think are likely to affect data privacy/data protection in the future? Is there anything else you would like to highlight?

As noted above, the DPDP Act has been enacted, but has yet to take effect. The Government will likely prescribe a phase-wise rollout of the provisions of the DPDP Act over a period of time. Once effective, the DPDP Act will serve as a comprehensive framework for data protection in India and envisages more robust requirements for the processing of personal data.

Indonesia

FIRM

Hutabarat Halim & Rekan (HHR Lawyers)
www.hhrlawyers.com

CONTACT

Milanti T. Kirana
Jakarta, Indonesia

Tel +6221 50913991
milantikirana@hhrlawyers.com

HHR Lawyers is a top-tier Indonesian commercial law firm with an eminent professional reputation. Since its establishment in 1996 by its two founding partners, Pheo M. Hutabarat and Nini N. Halim, HHR Lawyers has evolved and demonstrated its ability to provide superior legal works and client services, thus sustaining its ability to be one of the most reputable and leading commercial law firms in Indonesia with a global reach. With more than 26 years of experience, HHR Lawyers is fully supported by a number of experienced Indonesian lawyers and foreign legal consultants with skills across a broad range of commercial, corporate, finance, and commercial dispute matters.

HHR Lawyers provides a wide range of legal services to its clients. HHR Lawyers' expertise and capability have been acknowledged in various professional circles, namely: (i) capital market, banking and finance; (ii) commercial dispute resolutions; (iii) corporate, investment and M&A; (iv) energy and natural resources; (v) privatization and development; (vi) manpower and industrial relations; (vii) trade and competition; (viii) technology and intellectual property; (ix) tourism and real estate; (x) aviation; and (xi) shipping.

1. What are the major personal data protection laws or regulations in your jurisdiction? Is there any cross-sector legislation, and does it prevail over sector-specific legislation or vice versa?

The major personal data protection laws and/or regulations are the Indonesia Personal Data Protection Law No. 27 of 2022 ("PDP Law"), which was enacted in October 2022, and Ministry of Communication and Information Regulation No. 20 of 2016 ("MOCI Reg No. 20/2016"). The PDP Law covers both protection in electronic and non-electronic systems, while the MOCI Reg No. 20/2016 only covers protection in electronic systems. The PDP Law serves as a basic law that applies to every government body in Indonesia and is cross-sectoral in nature. However, there are also several sector-specific requirements, with a few examples as follows: (i) **Banking and digital financial services sector**: regulated under Financial Services Authority (Otoritas Jasa Keuangan) Regulation No. 12 of 2018; and (ii) **Health sector:** regulated under (i) Law No. 36 of 2009 on Health; and (ii) **Government Regulation** ("GR") No. 46 of 2014. The PDP Law in Indonesia is still pending various implementation. As such, we expect several adjustments in the near future.

2. Which regulatory authorities are responsible for the implementation and enforcement of personal information protection laws?

The Ministry of Communication and Information ("MOCI") is currently the regulatory authority on personal data ("PD") protection and has the authority to control cyber activities throughout Indonesia, provide regulations, and issue licenses for companies engaging in the information and technology sector.

The PDP Law introduces a new regulatory authority, i.e., "institution," whose main role is to actualize the implementation of PD protection. However, to date, the implementation of regulation on such institution has yet to be enacted.

3. How is "personal information"/"personal data" defined, and are there any categories of personal data that receive special or different protection (e.g., employees, minors, "sensitive" personal information, etc.)? If so, what are these categories, and can you summarize what special rules apply to these categories?

In general, Article 4 of the PDP Law provides two different categories of PD, as follows:

a. **Specific PD:** (i) data and information on health; (ii) biometric data; (iii) genetic data; (iv) criminal records; (v) data on children; (vi) personal financial data; and/or (vii) other data as stipulated under the laws and regulations.

b. **General PD:** (i) full name; (ii) gender; (iii) nationality; (iv) religion; (v) marital status; and/or (vi) combined PD to identify someone.

Article 25 and Article 26 of the PDP Law also acknowledge special personal data processing, i.e.:

a. **Processing of Children PD:** shall be carried out in special manners and there is an obligation to obtain consent from the parents and/or the guardian in accordance with the laws and regulations; and

b. **Processing of Persons with Disabilities PD:** shall be carried out in special manners through communication with specific methods in accordance with the laws and regulations, and there is an obligation to obtain consent from the person with disabilities and/or the guardian in accordance with the laws and regulations.

No explanation on the scope and implementation of "special manners" on personal data of children and persons with disabilities has been provided.

4. What are the key principles under the major personal data protection laws or regulations relating to personal data?

The principles of personal data protection are regulated under the PDP Law, as follows:

a. collection of PD is carried out on a limited and specific basis, in a way that is lawful and transparent;

b. processing of PD is carried out in accordance with its purposes;

c. processing of PD is carried out by guaranteeing the rights of the personal data subject;

d. processing of PD is carried out accurately, completely, not misleadingly, up-to-date, and accountably;

e. processing of PD is carried out by protecting the security of personal data against unlawful access, unlawful disclosure, unlawful alteration, misuse, destruction, and/or loss of personal data;

f. processing of PD is carried out through notifications on the purpose, activity, and failure of PD protection;

g. Personal data is destroyed and/or erased following the expiration of the retention period or upon the request from the PD subject, unless determined otherwise by the prevailing laws;

h. processing of PD is carried out responsibly and can be clearly proven.

5. Are there any formal registration compliance requirements that apply to all businesses (e.g., the appointment of data protection officers, registration of databases, etc.)?

PDP Law stipulates that all prevailing provisions related to the processing of PD are still in effect as long as such provisions are not in contradiction with the PDP Law. On this basis, the main provisions on registration with authorities are as stipulated under GR No. 71/2019 and MOCI Reg No. 5/2020 – wherein GR No. 71/2019 mandates that all Electronic System Providers ("ESP") are to conduct registration with the MOCI using the system of Online Single Submission.

PDP Law also mandates the appointment of an "officer" who carries out the functions of PD protection under certain circumstances, such as:

a. processing of PD for public service interest;

b. where the core activities of the PD Controller have a nature, scope, and/or purpose that require regular and systematic monitoring of PD on a large scale; and

c. where the core activities of the PD Controller comprise the PD processing on a large scale for a specific PD and/or PD related to a criminal offense.

6. What obligations are there for organizations to establish compliance programs (e.g., legal and operational policies, contracts, etc.) relating to the processing, use, and disclosure of personal data?

MOCI Reg No. 20/2016 provides that one of the principles of personal data protection is the existence of internal regulation on the processing of personal data. In relation to this, Article 35 (a) of the PDP Law states that the PD Controller is obligated to protect and ensure the safety of the processed personal data by way of preparation and implementation of operational technical steps to protect the PD against the interference of PD processing which violates the laws and regulations.

7. What restrictions, if any, are there on personal data being transferred to other jurisdictions? How would organizations generally address these restrictions?

Trans-border data flows are regulated under Article 56 of the PDP Law, with the following limitations:

a. In performing the PD transfer, the PD Controller shall ensure that the PD Controller and/or PD Processor who receives the transfer of PD has a PD protection level equal to or higher than the PDP Law;

b. In the event that the requirement under point (a) is not fulfilled, the PD Controller shall ensure an adequate and binding PD protection is in place;

c. In the event that the requirements under points (a) and (b) are not fulfilled, the PD Controller is obligated to obtain the consent of the PD subject.

To address these obligations and ensure compliance with these requirements, the relevant PD Controller is able to request advocacy from the MOCI (Art. 23 (2) (b) of MOCI Reg No. 20/2016).

8. What restrictions, if any, are there on using or re-using personal data for data analytics/innovation or in adopting new business solutions such as artificial intelligence or data analytics? How would organizations generally address these restrictions?

Article 10 of the PDP Law provides that the data subject has the right to object to decision-making measures based solely on automated processing, including profiling, which has legal consequences or a significant impact on the data subject. To ensure compliance with the foregoing, the PD Controller must provide detailed information on the use of the personal data, including the legal basis, prior to the provision of consent from the data subject. This way, the data subject will be fully informed on how their personal data will be used, minimizing the probability of consent withdrawal. An implementing regulation will be issued in respect of this matter.

9. What are the rights of an individual whose personal data is collected? Can they withdraw their consent, object to (and/or request deletion of) the retention of their personal data? If so, how?

PDP Law lists the following rights of data subjects:

a. obtain information on the clarity of identity, basic legal interest, purpose(s) of the request and use of PD, and accountability of the party who requests the PD;

b. complete, update, and/or correct the error and/or inaccuracy of the PD about themselves in accordance with the purpose of PD processing;

c. obtain access to and a copy of the PD about themselves in accordance with the prevailing laws;

d. end the processing, delete, and/or destroy PD about themselves in accordance with the prevailing laws;

e. withdraw the given consent on the processing of PD about themselves.

Data subjects also have the right to request: (i) termination of personal data processing; (ii) erasure of personal data; and/or (iii) destruction of personal data, by submitting a request to the PD Controller (Art. 42, 43, 44 of the PDP Law).

Note that there are several exemptions to the rights of the data subject, as follows:

a. national defense and security interests;

b. the interests of the law enforcement process;

c. public interest in the context of state administration;

d. the interests of supervision of the monetary financial services sector, payment systems, and financial system stability carried out in the context of state administration; or

e. the interests of statistics and scientific research.

10. Are there any penalties, liabilities, or remedies if any of the personal information protection laws are violated?

Yes, under the PDP Law, any violation and non-compliance with the provisions of PDP Law may be subject to the following sanctions:

a. administrative sanctions: (i) written notification; (ii) temporary suspension of the activities of personal data processing; (iii) erasure and/or destruction of personal data; and/or (iv) administrative fines – at a maximum two (2) percent of the annual receipt against the variables of violations;

b. criminal sanctions: imprisonment at a maximum of six (6) years and/or fines up to IDR 6 billion (for individuals) or fines, at ten (10) times the fines imposed (for corporations).

11. Is there mandatory data breach reporting in your jurisdiction? If so, could you summarize the thresholds that trigger reporting, what should be reported and to whom, and what timelines are required/expected?

Yes, in the event of failure in personal data protection, the Personal Data Controller must provide written notification, at the latest, within 72 hours to the personal data subject and institution – wherein such notification shall cover: (i) the disclosed personal data; (ii) when and how such personal data was disclosed; and (iii) measures of the Personal Data Controller to handle and recover the disclosed personal data. Additionally, in certain cases, such notification shall also include the public.

Further, pursuant to GR No. 71/2019, there is an obligation for the ESP to report to law enforcement and MOCI at the first opportunity when a system failure or disturbance occurs as a result of any party's action. The regulation is silent on when the report must be submitted.

12. Are there any recent notable developments in your country or cases that you think are likely to affect data privacy/data protection in the future? Is there anything else you would like to highlight?

A personal data breach happened recently in May 2023. A financial institution company suffered from a cyberattack, with the leak totaling 1.5 terabytes. In response to this incident, the company decided to spend additional money on its IT capital expenditure and changed the structure of its board of directors. This shows how crucial it is to speed up the enaction of the implementation of regulations of the PDP Law.

Japan

FIRM

Kojima Law Offices
www.kojimalaw.jp/en/

CONTACT

Nozomi Watanabe
Tokyo, Japan

Tel +81 3 3222 1401
watanabe@kojimalaw.jp

Kojima Law Offices ("KLO") handles all types of commercial transactions and corporate legal matters, including assisting American, European, and other foreign corporations and individuals with inbound investments. We guide our clients through the intricacies of doing business in Japan's unique legal and business culture.

KLO assists clients in a broad range of areas, including Foreign Direct Investment ("FDI") for Japan-bound investors. For nearly four decades, KLO has guided a wide variety of foreign clients – from an international beverage company to foreign governments to start-up businesses – to successfully establish operations in Japan. In the early 1990s, KLO was the first law firm to establish a legal mechanism to assist Japanese companies investing in India. KLO has extensive experience establishing joint ventures, creating strategic alliances, and handling mergers and acquisitions. We work with foreign companies to solve day-to-day problems, including regulatory compliance and employment issues.

With its strong litigation department, KLO has represented foreign governments before the Japanese courts and has extensive experience representing both Japanese and foreign clients in international arbitrations.

1. What are the major personal data protection laws or regulations in your jurisdiction? Is there any cross-sector legislation, and does it prevail over sector-specific legislation or vice versa?

Japan's main personal information protection law is the Act on the Protection of Personal Information ("APPI"), along with both its accompanying general guidelines and specific guidelines. The specific guidelines cover the following seven business areas:

(i) financial services;

(ii) medical services;

(iii) telecommunications;

(iv) broadcasting;

(v) postal services provided by Japan Post;

(vi) letter delivery services; and

(vii) personal genetic information.

An entity that provides any of the seven services in Japan will therefore need to comply with the Act itself, the general guidelines, and the specific guidelines. The APPI is itself a piece of cross-sector legislation, and the sector specific guidelines mentioned above merely interpret the APPI.

2. Which regulatory authorities are responsible for the implementation and enforcement of personal information protection laws?

The Personal Information Protection Commission ("PPC") has the exclusive authority to handle matters involving the protection of personal information (see https://www.ppc.go.jp/en/ for information on the PPC and the APPI, including both the general and specific guidelines discussed above).

3. How is "personal information"/"personal data" defined, and are there any categories of personal data that receive special or different protection (e.g., employees, minors, "sensitive" personal information, etc.)? If so, what are these categories, and can you summarize what special rules apply to these categories?

The Act defines "personal information" as either:

(i) information about a living individual that contains a name, date of birth, or other description that can identify a person (including separate pieces of information that can collectively identify an individual); or

(ii) information containing the unique individual identification number that the government issues to all residents of Japan (this is analogous to social security numbers in the US).

The "other description" in (i) means anything stated, recorded, or otherwise expressed through voice, motion, or other methods in a document, a drawing, or in electronic form.

Because the Act specifically applies to "living individuals," it does not protect information of the deceased, nor does it protect a corporation's information. On the other hand, because the Act covers information that can identify a specific individual, the Act may, under certain circumstances, protect fingerprints, irises, and specific DNA sequences as personal information.

An example of how separate pieces of information can collectively identify an individual can be seen in the unique numbers that some companies assign to their customers as part of the product registration process (such as "W2P99N" instead of "Yukio Nishima" discussed below). When customers register products with a company, they typically provide the company with certain information such as their name, address, and telephone number. Many companies use this information to create a customer database to notify customers about new products or special offers. Because this unique number is linked to the customer's personal information, the Act considers the number itself to be personal information.

The Act recognizes certain categories of personal data that are subject to different protections. One such category is called "sensitive personal information," which requires an individual's prior consent before it can be obtained. This information concerns a person's race, religion, ideology, social status, medical history, criminal record, or the fact that one has been the victim of a crime. The "social status" category is intended to protect certain groups of people in Japan who have historically faced unique forms of discrimination as a result of being born into a certain class.

The Act recognizes an additional category of personal data called "anonymized personal information" that is subject to different protections. This information relates to an individual but has been modified so that it is no longer possible to identify that individual (meaning that it is technically not personal information anymore). An example is the following data, which a company uses in conjuction with each other: (1) changing a customer's name to a random string of letters and numbers ("W2P99N" instead of "Yukio Nishima"); (2) using an age range instead of the customer's date of birth ("30-40 years old" vs. "April 11, 1989"); and (3) using just the city where the customer lives instead of the customer's address ("Tokyo" instead of "1-2-3 Nihonbashi Street"). Businesses are allowed to transfer anonymized personal information so long as they make public the kinds of personal information included in the anonymized personal information.

Similar to anonymized personal information, the Act also recognizes a category of personal data called "pseudonymized personal information." This is information that relates to an individual but has been modified so that it is not possible to identify that individual without additional data. Pseudonymized personal information can be used internally to improve business operations, and entities are permitted to retain pseudonymized personal information for future analysis. However, because this information remains "personal data" under the APPI, the law still applies a number of restrictions to businesses that possess pseudonymized personal information. Specifically, a business will face greater restrictions if it possesses other pieces of personal information that can be combined with the pseudonymized personal information to allow the identification of the individual.

Lastly, the 2020 Amendments also introduced personally referable information, which includes data such as cookies and purchase history. Businesses must obtain a data subject's consent (typically in an opt-in, pop-up window) in order to transfer this data to a third party who will combine this data with other data and convert it to personal information. To transfer personally referable information overseas, the transferring operator must also explain to the data subject the data protection system of both the overseas country and the recipient of the data.

4. What are the key principles under the major personal data protection laws or regulations relating to personal data?

The key principle of the Act is balancing the obvious usefulness of personal information with the need to protect it. This balance is evident in the Act itself. For example, the Act acknowledges that the use of personal information can be helpful in providing society with a variety of useful goods and services. At the same time, the Act recognizes that in an advanced information society, there is a risk of serious human rights violations resulting from the improper use of personal information.

5. Are there any formal registration compliance requirements that apply to all businesses (e.g., the appointment of data protection officers, registration of databases, etc.)?

No, there are no formal registration compliance requirements that apply to all businesses. Businesses simply need to take adequate security measures to protect personal information under the APPI; they do not need to take specific measures such as appointing data protection officers or registering databases.

6. What obligations are there for organizations to establish compliance programs (e.g., legal and operational policies, contracts, etc.) relating to the processing, use, and disclosure of personal data?

The APPI requires that businesses establish systematic security control measures, personnel safety control measures, physical security control measures, and technical safety control measures to protect the personal data they handle.

7. What restrictions, if any, are there on personal data being transferred to other jurisdictions? How would organizations generally address these restrictions?

An organization must obtain the data subject's consent before it can transfer the data to another jurisdiction unless the transfer:

(i) is required by Japanese law/regulations;

(ii) is necessary to prevent death, injury, or property damage, and it is difficult to obtain the individual's consent;

(iii) is necessary to improve public health or to promote the welfare of children, and it is difficult to obtain the individual's consent; or

(iv) is made to a jurisdiction white-listed by the PPC, or is made to a jurisdiction with at least as robust data protection standards as the APPI, but only in certain situations, such as when the processing of personal information is outsourced, the personal information is being transferred as a part of a business takeover, and when personal information is shared among group companies.

8. What restrictions, if any, are there on using or re-using personal data for data analytics/innovation or in adopting new business solutions such as artificial intelligence or data analytics? How would organizations generally address these restrictions?

Organizations can use the pseudonymously processed information discussed in Question 3 for internal purposes such as data analytics and developing new computational models. Unlike other forms of data, businesses are allowed to use pseudonymously processed information beyond the original purpose that the data subject consented to, and they can retain it for future data analytics purposes. Data subjects have the right to request that businesses delete their personal information after the business is done using it.

9. What are the rights of an individual whose personal data is collected? Can they withdraw their consent, object to (and/or request deletion of) the retention of their personal data? If so, how?

The Act gives individuals the right to require a company to:

(1) disclose any personal information that the company has on them;

(2) correct any erroneous information; and

(3) stop using, delete, and/or stop transferring any personal information that the company is handling in violation of the Act or if the company no longer needs to use the information. An individual can also require a business to stop using or delete their personal information if the business suffers a data breach or if there is otherwise a threat to their data rights.

Apart from item (3) above (which arguably serves as a "withdrawal of consent"), the APPI does not explicitly allow an individual to withdraw their consent.

10. Are there any penalties, liabilities, or remedies if any of the personal information protection laws are violated?

The maximum punishment for violating the Act is ¥100 million for a business and ¥1 million or up to a year imprisonment for an individual. In practice, however, fines are rare and prison sentences are even more uncommon unless one wilfully and repeatedly refuses to comply. Japanese authorities typically first issue "administrative guidance" to violators, especially first-time violators. This administrative guidance is essentially a warning, as the authorities generally avoid imposing penalties without first giving the violator a chance to resolve any issues that caused the violation. Typically, only if the violator fails to comply with the administrative guidance do the authorities impose penalties.

11. Is there mandatory data breach reporting in your jurisdiction? If so, could you summarize the thresholds that trigger reporting, what should be reported and to whom, and what timelines are required/expected?

Yes, the APPI has mandatory data breach reporting under certain circumstances. Specifically, businesses must submit a preliminary report to the PPC promptly following a breach if the impacted data includes sensitive data, if the data is likely to be used unlawfully and will result in financial damage, if the breach was committed maliciously, or if more than 1,000 subjects will likely be impacted by the data breach. The APPI also requires businesses that suffer a data breach to either inform the impacted individuals or, if that is too difficult, to make a public announcement and set up a way for impacted data subjects to contact the business and have their concerns addressed.

12. Are there any recent notable developments in your country or cases that you think are likely to affect data privacy/data protection in the future? Is there anything else you would like to highlight?

The most recent amendments to the APPI went into full effect on April 1, 2022, and the law is generally reviewed and amended every three years to address changes in technology. Therefore, we may see revisions to the APPI over the next few years, perhaps to better address the recent focus on AI and large language models.

Further, the EU Commission has recognized Japan as a jurisdiction that meets the adequacy requirements for transfers of personal data from the EU, paving the way for easier transfers of personal data between the two jurisdictions.

Korea

FIRM

K1 Chamber LLP
https://en.k1chamber.com

CONTACT

Jong Jae Lee
Seoul, South Korea

Tel +82 26956 8420
jjlee@k1chamber.com

K1 Chamber LLP was established in May 2021, with the vision of becoming a cutting-edge law firm that could offer a truly premier service in a timely, innovative, and strategic way. We have an integrated team of highly regarded experts and industry leaders in our selected fields, covering a broad range of practices and sectors including financial services, IP/IT, privacy & personal information protection, pharmaceuticals, digital economy, corporate, commercial, real estate and global disputes. In relation to privacy and personal information protection, our partners have expertise in Korean data privacy and data security laws, such as the Personal Information Protection Act and other laws that have a bearing on information security and data protection and will be available to assist our client to better understand the extensive Korean privacy and personal information protection requirements. We are part of the Meritas international network of law firms. K1 Chamber is committed to delivering its promise to be our clients' most trusted advisors, proactively identifying issues and creatively formulating strategic solutions through collaboration with a seamless team of experts both internally and externally.

1. What are the major personal data protection laws or regulations in your jurisdiction? Is there any cross-sector legislation, and does it prevail over sector-specific legislation or vice versa?

In Korea, the major personal data protection laws and regulations are the Personal Information Protection Act (the "PIPA") and the Act on Promotion of Information and Communications Network Utilization and Information Protection (the "Network Act"). These laws aim to safeguard the privacy and rights of individuals regarding their personal information.

The PIPA is a comprehensive law that applies to all sectors and sets out general principles and requirements for personal data protection. It serves as a baseline for personal data protection across different industries. In addition to the PIPA, there are also sector-specific laws and regulations that may supplement the general provisions of the PIPA. These sector-specific laws apply to specific industries or areas, such as financial services, healthcare, telecommunications, and credit reporting. While sector-specific laws provide additional regulations for those specific industries, they should be read in conjunction with the PIPA. In case of any conflicts or inconsistencies, the sector-specific laws must comply with the general principles and requirements set forth by the PIPA.

2. Which regulatory authorities are responsible for the implementation and enforcement of personal information protection laws?

In Korea, the Ministry of the Interior and Safety (the "MOIS") is responsible for the overall supervision and coordination of personal data protection. The Korea Communications Commission (the "KCC") is responsible for the enforcement of the Network Act, which includes provisions on personal data protection in the context of electronic communications. The Korea Personal Information Protection Commission (the "PIPC") is the central administrative agency responsible for the implementation and enforcement of the PIPA, including the development of guidelines and regulations, handling of complaints and disputes, and imposition of administrative fines and penalties in case of non-compliance. Other sector-specific regulators may also play a role in enforcing personal data protection regulations in their respective industries.

3. How is "personal information"/"personal data" defined, and are there any categories of personal data that receive special or different protection (e.g., employees, minors, "sensitive" personal information, etc.)? If so, what are these categories, and can you summarize what special rules apply to these categories?

In Korea, personal information is defined as any information that can identify a specific individual, including but not limited to name, resident registration number, photograph, fingerprints, and personal identification number. Under the PIPA, there are certain categories of personal data that receive special protection. First, there is certain sensitive personal information, which includes information about race, ethnicity, ideology, creed, political inclination, labor union membership, health status, sexual orientation, DNA information acquired from genetic testing, data that constitutes a criminal history, personal information resulting from specific technical processing of data relating to the physical and physiological or behavioral characteristics of an individual for the purpose of uniquely identifying that individual.

This type of data requires a higher level of protection, and explicit consent is generally required for its collection, use, and disclosure. Personal information of children under the age of 14 is also subject to additional safeguards, including the requirement for parental or legal guardian consent.

4. What are the key principles under the major personal data protection laws or regulations relating to personal data?

In Korea, the key principles under the PIPA and the Network Act are as follows:

First, personal data should be collected and used only for specific and legitimate purposes, and individuals should be informed of the purpose of data collection.

Next, generally, the consent of individuals is required for the collection, use, and disclosure of their personal data. Consent should be obtained in a clear and voluntary manner, and individuals have the right to withdraw their consent.

Next, personal data should be collected and processed in a minimal and necessary manner for the intended purpose. Excessive collection and retention of personal data is generally prohibited.

Next, organizations are required to implement appropriate technical and administrative measures to protect personal data from unauthorized access, alteration, disclosure, or destruction.

Lastly, individuals have various rights, including the right to access their personal data, the right to request correction or deletion of inaccurate or outdated data, and the right to object to the processing of their data in certain circumstances.

5. Are there any formal registration compliance requirements that apply to all businesses (e.g., the appointment of data protection officers, registration of databases, etc.)?

In Korea, there are formal registration and compliance requirements related to personal information for businesses. Here are some key compliance requirements:

Certain organizations, such as those processing large volumes of personal information or engaged in specific types of data processing activities, are required to appoint a Data Protection Officer (the "DPO"). The DPO is responsible for overseeing and ensuring compliance with personal information protection regulations. Under the PIP, organizations are required to register their databases with the PIPC if they meet certain criteria, such as processing sensitive personal information or having a certain number of data subjects. Organizations are also required to implement appropriate technical and administrative measures to protect personal information from unauthorized access, loss, alteration, or disclosure.

6. What obligations are there for organizations to establish compliance programs (e.g., legal and operational policies, contracts, etc.) relating to the processing, use, and disclosure of personal data?

Organizations are required to establish and maintain compliance programs related to the processing, use, and disclosure of personal data. The PIPA requires businesses to develop and implement policies and procedures to protect personal information, including the establishment of a privacy policy that outlines how personal information is collected, used, and disclosed. Organizations are also required to enter into data protection agreements with third-party service providers that process personal information on their behalf. These agreements must specify the purpose and scope of the processing, the measures taken to protect personal information, and the obligations of the service provider.

7. What restrictions, if any, are there on personal data being transferred to other jurisdictions? How would organizations generally address these restrictions?

In Korea, the transfer of personal data to other jurisdictions is available in certain circumstances specifically provided in the PIPA. Under the PIPA, such circumstances where the personal information can be transferred overseas

are: (1) when separate consent to the transfer of the personal information overseas has been obtained from the data subject; (2) when it is necessary to outsource the processing of or storing of the personal information to execute and enforce the agreement with the data subject; (3) when the party receiving the personal information is accredited by the PIPC; and (4) when the country where the personal information is transferred is deemed to have an adequate level of data protection by the Korean government.

8. What restrictions, if any, are there on using or re-using personal data for data analytics/innovation or in adopting new business solutions such as artificial intelligence or data analytics? How would organizations generally address these restrictions?

In Korea, organizations need to obtain consent from individuals before collecting and using their personal data for such purposes. They must also adhere to principles of purpose limitation, data minimization, and de-identification when handling personal data.

To address these restrictions, organizations usually implement measures such as consent management, anonymization and de-identification, data security measures, privacy impact assessments, compliance frameworks, etc.

9. What are the rights of an individual whose personal data is collected? Can they withdraw their consent, object to (and/or request deletion of) the retention of their personal data? If so, how?

In Korea, individuals have rights regarding the collection and handling of their personal data. They have the right to withdraw their consent, object to the retention of their personal data, and request deletion of their personal data under certain circumstances. To withdraw consent or object to retention of their personal data, it is necessary to submit a request after clearly stating the intention to withdraw consent, object to retention, or request deletion of their personal data and provide relevant details such as name, contact information, and any specific personal data it wishes to address.

10. Are there any penalties, liabilities, or remedies if any of the personal information protection laws are violated?

In Korea, there are penalties, liabilities, and remedies in place if personal information protection laws are violated. Here are some key penalties:

1. Administrative Penalties: The PIPC has the authority to impose administrative fines for violations of the PIPA. Depending on the severity of the violation, fines can range from 3 million Korean won (approximately $2,500) to 5% of the annual revenue of the violating entity.

2. Criminal Penalties: In cases of serious breaches, intentional violations, or illegal transfers of personal information, criminal penalties may be imposed. Individuals found guilty of such offenses can face imprisonment for up to five years or fines of up to 50 million Korean won (approximately $42,000).
3. Compensation for Damages: Individuals who suffer damages as a result of a violation of their personal information rights may seek compensation through civil lawsuits. This can include financial compensation for any harm caused by the violation.
4. Corrective Measures: The PIPC can order organizations to take corrective actions, such as halting the collection or use of personal information, implementing security measures, or conducting internal audits to ensure compliance.

11. Is there mandatory data breach reporting in your jurisdiction? If so, could you summarize the thresholds that trigger reporting, what should be reported and to whom, and what timelines are required/expected?

There is mandatory data breach reporting in Korea. Under the PIPA, organizations must report data breaches if they involve sensitive personal information (including resident registration numbers, passwords, financial information, etc.) of 1,000 or more individuals. When a data breach occurs, organizations must report the following information: nature of the breach, measures taken or planned to mitigate the damage, and measures taken or planned to prevent future breaches. Data breaches should be reported to the PIPC and the affected individuals. If the breach affects more than 1,000,000 individuals, additional notification through public announcements may be required. Data breaches must be reported without undue delay once they are confirmed. However, specific timelines are not mentioned in the law.

12. Are there any recent notable developments in your country or cases that you think are likely to affect data privacy/data protection in the future? Is there anything else you would like to highlight?

One recent notable event is the new amendment to the PIPA with respect to the transfer of personal information overseas. Under the new amendment enacted on March 14, 2023, and enforceable from September 15, 2023, the transfer of the personal information overseas is made possible without procuring the consent of the data subject. As such, consent would not be required for transfer of personal information overseas to a party that is accredited by the PIPC and to a country that is deemed to have an adequate level of data protection by the Korean government.

There have also been several high-profile data breaches and privacy incidents in Korea in recent years which have raised public awareness and concerns about data protection. These incidents have prompted discussions and calls for stricter regulations and enforcement.

Further, Korea has been recognized by the EU Commission as a jurisdiction that meets adequacy requirements for transfers of personal data from the EU, paving the way for easier transfers of personal data between the two jurisdictions.

Overall, these developments indicate a growing emphasis on data privacy and protection in Korea, and we can expect further advancements and measures to safeguard personal information in the future.

Malaysia

FIRM

Zul Rafique & Partners
www.zulrafique.com.my

CONTACT

Yit Meng Kor
Kuala Lumpur, Malaysia

Tel +603 6209 8247
darren@zulrafique.com.my

Zul Rafique & Partners (ZRp) is a Kuala Lumpur-based law firm that was formed in December 1999. As a result of significant growth achieved since its inception, ZRp is now a large, broad-based commercial legal practice.

We have strategically focused our talents into specialized practice groups to maximize the depth of our expertise and experience. Our expanding practice takes this into account, and in our lawyers you will find impeccable legal foundation which complements a diversity of shared experiences and specialist skills.

Our Practice Groups include:

- Banking & Finance
- Capital Markets
- Communications & Multimedia
- Construction Dispute Resolution
- Corporate Liability & Risk Management
- Corporate/Mergers & Acquisitions
- Corporate Real Estate
- Employment & Industrial Relations
- Energy & Utilities
- Infrastructure & Construction
- Intellectual Property
- Legal Forensic Investigation & Compliance
- Litigation
- Oil & Gas
- Projects & Corporate Advisory
- Tax

1. What are the major personal data protection laws or regulations in your jurisdiction? Is there any cross-sector legislation, and does it prevail over sector-specific legislation or vice versa?

In Malaysia, the primary legislation governing personal data protection is the Personal Data Protection Act 2010 ("PDPA") and its subsidiary regulations. The PDPA applies to:

(i) any person who processes; and

(ii) any person who has control over or authorizes the processing of, any personal data in respect of commercial transactions.

Under Section 23 of the PDPA, a code of practice may be issued and registered to regulate personal data matters for a class of data users. A code of practice may be prepared by a data user forum designated by the Personal Data Protection Commissioner ("PDP Commissioner") or be issued by the PDP Commissioner under certain circumstances. A code of practice only takes effect upon registration in the Register of Codes of Practice. Section 29 of the PDPA mandates data users' compliance with the code of practice, otherwise a fine and/or imprisonment may ensue.

The General Code of Practice of Personal Data Protection is a registered code that applies to a class of data users who have not prepared a code of practice and/or where there is no data user forum to develop the relevant code of practice for a particular class of data users. Separately, there are sector-specific codes of practice developed by data user forums which deal with the sector-specific data protection requirements.

Protection of customer data (which may include personal data) is also regulated by sector-specific legislation and must be complied with alongside the PDPA. Relevant sectors include banking and finance, healthcare, and telecommunications.

2. Which regulatory authorities are responsible for the implementation and enforcement of personal information protection laws?

The Minister of Communications and Digital ("Minister") regulates matters relating to PDPA, while the PDP Commissioner appointed by the Minister carries out the functions and powers assigned to them under the PDPA.

The functions and powers of the two authorities are clearly separated and defined under the PDPA.

3. How is "personal information"/"personal data" defined, and are there any categories of personal data that receive special or different protection (e.g., employees, minors, "sensitive" personal information, etc.)? If so, what are these categories, and can you summarize what special rules apply to these categories?

Personal data under the PDPA means any information, in respect of commercial transactions, which:

(i) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;

(ii) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or

(iii) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

that relates directly or indirectly to a data subject, who is identified or identifiable from that and other information in the possession of a data user in respect of commercial transactions, including any sensitive personal data and expression of opinion about the data subject. Note that information processed for a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010 is excluded by the definition of personal data in the PDPA.

The PDPA also defines specific personal data categories—namely, "sensitive personal data" consisting of the data subject's information regarding their health and beliefs, the commission or alleged commission of offenses, or other personal data gazetted by the Minister. A data user shall not process "sensitive personal data" unless:

(i) there is explicit consent;

(ii) an exception for explicit consent is fulfilled; or

(iii) the information has been made public as a result of steps deliberately taken by the data subject.

Another sub-category is personal data relating to data subjects who are under eighteen years old. Consent from the parent or guardian of the data subject must be obtained to process such personal data.

4. What are the key principles under the major personal data protection laws or regulations relating to personal data?

Seven key principles are prescribed under the PDPA:

(i) General Principle - consent must be obtained from data subjects before processing their personal information unless exempted, and the

processing shall be for lawful purposes, adequate, relevant, and not excessive;

(ii) Notice and Choice Principle – to inform the data subject on how their personal data is processed;

(iii) Disclosure Principle – no disclosure of personal data for purposes other than that disclosed at the time of collection or to any party other than those disclosed in the data protection notice;

(iv) Security Principle – to ensure adequate security measures to protect personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration, or destruction;

(v) Retention Principle – personal data shall not be kept longer than necessary to fulfil the relevant purpose;

(vi) Data Integrity Principle – to ensure personal data is accurate, complete and up to date; and

(vii) Access Principle – data subject has rights to access and correct their personal data.

5. Are there any formal registration compliance requirements that apply to all businesses (e.g., the appointment of data protection officers, registration of databases, etc.)?

The formal registration compliance requirement is only applicable for data users who belong to the class of data users prescribed in the Personal Data Protection (Class of Data Users) Order 2013 (as amended) where such data user is required to register with the PDP Commissioner.

6. What obligations are there for organizations to establish compliance programs (e.g., legal and operational policies, contracts, etc.) relating to the processing, use, and disclosure of personal data?

Each organization must establish a compliance program to ensure compliance with the seven personal data protection principles and, where applicable, the relevant codes of practice. Additionally, such compliance program must comply with the standards required by the Personal Data Protection Standard 2015 ("Data Protection Standard"). The Data Protection Standard prescribes minimum requirements on security, retention, and data integrity standards relating to personal data.

7. What restrictions, if any, are there on personal data being transferred to other jurisdictions? How would organizations generally address these restrictions?

Section 129 of the PDPA prohibits the transfer of personal data outside of Malaysia by data users, unless to a country gazetted by the Minister ("whitelist arrangement"). Notwithstanding this general prohibition, a data user may transfer personal data to a place outside of Malaysia provided the transfer falls within an exception enshrined in Section 129, including (without limitation) where the data subject has given consent to the transfer, or the transfer is necessary for the conclusion or performance of a contract.

The Public Consultation Paper No. 01/2020 ("PCP No. 01/2020") published by the PDP Commissioner recommended the removal of this whitelist arrangement and for Section 129 of the PDPA to be restructured to provide clear conditions allowing for transfers of personal data to places outside Malaysia. The PCP No. 01/2020 acknowledges that this is essential to facilitate e-commerce transactions and free trade agreements.

8. What restrictions, if any, are there on using or re-using personal data for data analytics/innovation or in adopting new business solutions such as artificial intelligence or data analytics? How would organizations generally address these restrictions?

Organizations must ensure that appropriate consents are obtained from data subjects to process personal data for such purposes. If no such consent was given when the data subject was first asked to provide their personal data or when the data user first collects the personal data of the data subject, the data subject's consent must be sought for such further processing of the personal information.

Alternatively, the data user may consider processing anonymized data to prevent any personal data from being processed and/or disclosed.

9. What are the rights of an individual whose personal data is collected? Can they withdraw their consent, object to (and/or request deletion of) the retention of their personal data? If so, how?

The PDPA confers the following rights to data subjects:

(i) access to personal data (Section 30);

(ii) to correct personal data (Section 34);

(iii) to withdraw consent to the processing of personal data (Section 38);

(iv) to prevent processing likely to cause damage or distress (Section 42); and

(v) to prevent processing for purposes of direct marketing (Section 43).

The data subject may exercise its rights above by giving written notice to the data user under the respective sections of the PDPA along with payment of the prescribed fees. Data users, upon receipt of the notice, are required by the PDPA to comply with the data subject's request unless it can provide reasons on why it is unable to do so. This exception does not apply to Section 43 of the PDPA, which mandates data users to comply with such written requests. The PDPA does not provide for a data subject's right to delete personal data retained by a data user under Section 44 of the PDPA, which requires the data user to keep and maintain information relating to personal data that has been or is being processed by the data user.

10. Are there any penalties, liabilities, or remedies if any of the personal information protection laws are violated?

Contravention of the PDPA (including personal data protection principles) constitutes an offense for which fines and imprisonment may be applicable. For example, if Section 5 of the PDPA is contravened, upon conviction, the data user will be liable to a fine not exceeding RM300,000, imprisonment not exceeding two years, or both. The list of offenses set out by the Department of Personal Data Protection can be accessed via its website.

11. Is there mandatory data breach reporting in your jurisdiction? If so, could you summarize the thresholds that trigger reporting, what should be reported and to whom, and what timelines are required/expected?

The PDPA does not compel data users to notify or report any data breach incident.

However, such reporting was proposed to be made mandatory under the PCP No. 01/2020.

12. Are there any recent notable developments in your country or cases that you think are likely to affect data privacy/data protection in the future? Is there anything else you would like to highlight?

Recent notable developments include the PCP No. 01/2020 published in 2020 to obtain feedback from interested parties on new features or provisions to be incorporated into the PDPA. It offers insight into Malaysia's policy direction in relation to new development or features which may be introduced to the personal data protection obligations under the PDPA.

Some suggested features in the PCP No. 01/2020 include:

(i) appointment of a compliance officer;

(ii) right to be forgotten, i.e., right to obtain the erasure of personal data;

(iii) right to data portability, i.e., right to obtain their data in structured and machine-readable format and to transmit to other data users;

(iv) data protection by design, i.e., the requirement to implement appropriate technical and operational measures which are designed to implement the data protection principles;

(v) notification of personal data breaches;

(vi) implementation of a Do Not Call Registry;

(vii) imposing obligations on data processors directly, including implementing appropriate technical and organization measures, data breach notification, and maintaining a record of categories of processing activities; and

(viii) extending the application of the PDPA to the Federal and State Government.

If these new features are introduced into the PDPA, the PDPA would be more in line with the European Union General Data Protection Regulation. However, it would be a big shift for existing organizations (especially small and medium size organizations) who would likely require more time and budget to comply with these requirements.

In light of the recent data breach incident of the Malaysian COVID-19 tracing app, MySejahtera, the Minister of Communications and Digital emphasized the inadequacies of the PDPA, including the fines imposed for data breach incidents. The Minister has indicated that his Ministry is looking to improve proposed PDPA amendments by previous administrations and is targeting to present the amendments in Parliament before the end of 2023.

Philippines

FIRM

ACCRALAW
www.accralaw.com

CONTACT

John Paul M. Gaba
Metro Manila, Philippines

Tel +63 2 88308000
jmgaba@accralaw.com

Angara Abello Concepcion Regala & Cruz Law Offices (ACCRALAW) is a leading full-service firm with about 170 lawyers. Its main offices are located at the ACCRALAW Tower in the newly developed Bonifacio Global City in Metro Manila. It has full-service branches in the thriving commercial centers of Cebu City in the Visayas and Davao City in Mindanao. The firm has an excellent track record in handling diverse, significant, and complex business projects and transactions for both local and multinational clients and has been involved in landmark litigation cases. ACCRALAW's clientele represents the full spectrum of business and industry and includes professional organizations and individuals. Servicing the firm's clients are seven practice departments and its two branches, which offer timely, creative, and strategic legal solutions matched with cost-efficient administration and expert handling of clients' requirements.

1. What are the major personal data protection laws or regulations in your jurisdiction? Is there any cross-sector legislation, and does it prevail over sector-specific legislation or vice versa?

The governing law is the Data Privacy Act of 2012 or Republic Act No. 10173 ("DPA"), and its Implementing Rules and Regulations ("IRR"). The National Privacy Commission also issues circulars and advisories that further flesh out and implement the provisions of the DPA and its IRR.

2. Which regulatory authorities are responsible for the implementation and enforcement of personal information protection laws?

The lead agency that oversees the implementation of our local personal information privacy law and regulations is the National Privacy Commission ("NPC").

3. How is "personal information"/"personal data" defined, and are there any categories of personal data that receive special or different protection (e.g., employees, minors, "sensitive" personal information, etc.)? If so, what are these categories, and can you summarize what special rules apply to these categories?

"Personal information" is defined as any information, whether recorded in a material form or not, from which the identity of an individual is apparent by the entity holding the information. Information pertaining to juridical entities (such as corporations, companies, and partnerships) are not covered by the DPA, although records or documents of juridical entities may well contain personal information, and the portions of such records or documents should be treated as covered by the DPA.

Our law carves out two "special" sets of personal information – "Sensitive Personal Information" and "Privileged Information."

"Privileged Information" is defined as "any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication." Under Rule 130, Section 24 of our Rules of Court, the following constitute "privileged communication": (1) marital or spousal communication; (2) lawyer-client communication; (3) doctor-patient communication; (4) priest-penitent communication; and (5) public official communication.

"Sensitive Personal Information" refers to personal information:

(1) about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political affiliations;

(2) about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

(3) issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or their denials, suspension or revocation, and tax returns; and

(4) specifically established by an executive order or an act of Congress to be kept classified.

Under the DPA, both "Privileged Information" and "Sensitive Personal Information" are treated the same.

4. What are the key principles under the major personal data protection laws or regulations relating to personal data?

Similar to the principles of the EU GDPR, "processing of personal information" must adhere to the general principles of transparency, legitimate purpose, and proportionality. For example, if the personal data is collected for raffle draw, then the data subject must be informed that his data is being collected, processed, and retained only for the purpose and only as long as necessary to fulfill the contest requirements. The data must not be used for any other purpose or kept longer than necessary. The data collected must also be proportionate to the purpose declared to the data subject. The hallmark of the principle of transparency under the DPA is the need to have either the clear, expressed consent of the data subject or a valid legal ground for the processing of personal information. Primarily, the data subject must be informed as to how his personal information will be used or "processed" – who are the parties involved (e.g., data controllers, data processors, third parties), the purposes for which such personal information is needed, how long personal information shall be maintained, appropriate security measures being implemented to protect the data, and contact details as to how the data subject can reach out to the data controller in case he has any concerns. Absent any of the foregoing, "processing of personal information" can be generally considered as unauthorized under the DPA.

5. Are there any formal registration compliance requirements that apply to all businesses (e.g., the appointment of data protection officers, registration of databases, etc.)?

Generally, Personal Information Controllers ("PIC") and Personal Information Processors ("PIP") are required to appoint a Data Protection Officer ("DPO"). PICs and PIPs are required to register their DPO and their data processing systems ("DPS") with the NPC if they:

(1) employ at least two hundred fifty (250) employees; or

(2) undertake operations or personal information processing activities which are likely to pose a risk to the rights and freedoms of the data subjects, or such processing is not occasional, regardless of the number of employees; or

(3) process sensitive personal information of at least one thousand (1,000) individuals; or

(4) (regardless of the number of employees or data subjects) belong to industries which the NPC classifies as "critical sectors", e.g., banks and non-bank financial institutions; hospitals, medical centers, and health-related organizations; schools and universities; research institutions; business process outsourcing companies (including those acting as "shared service" providers or have a "captive market"); telecommunication companies.

6. What obligations are there for organizations to establish compliance programs (e.g., legal and operational policies, contracts, etc.) relating to the processing, use, and disclosure of personal data?

All PICs and PIPs must implement appropriate and reasonable security measures to ensure protection of the "confidentiality, integrity, and availability" of personal information. There are three (3) groups of measures: (1) organizational; (2) physical; and (3) technical security measures.

Organizational security measures include:

(1) designation of a DPO;

(2) creation of data protection policies which provide for organizational, physical, and technical security measures;

(3) maintenance of records that sufficiently describe its data processing system and identify the duties of individuals who have access to personal data;

(4) conducting of capacity building and training programs for employees who have access to personal data regarding privacy or security policies;

(5) development and implementation of procedures for collecting and processing personal data, access management, system monitoring, and protocols to follow during security incidents or technical problems, for data subjects to exercise their rights, and for a data retention schedule; and

(6) ensuring contracts with PIPs (i.e., third-party vendors) also implement the security measures required by the DPA and its IRR.

Physical security measures include:

(1) establishing policies/procedures to monitor and limit access to, and activities in, rooms, workstations or facilities (including guidelines on use of and access to electronic media);

(2) designing office space and workstations to ensure the privacy of processors of personal data;

(3) defining a clear description of duties, responsibilities, and work schedules to processors of personal data to ensure only individuals actually performing duties are in the room at the given time;

(4) implementing policies and procedures on the transfer, removal, disposal, and re-use of electronic media; and

(5) establishing policies and procedures on the prevention of the mechanical destruction of files and equipment.

Technical security measures include:

(1) establishing a security policy with respect to processing personal data;

(2) establishing safeguards to protect computer networks against unauthorized access or to ensure data integrity and functioning of the system;

(3) ensuring and maintaining the confidentiality, integrity, availability, and resilience of their processing systems and services;

(4) conducting regular monitoring for security breaches, accessing vulnerabilities, and preventive, corrective, and mitigating action against data breach;

(5) developing a capability to restore availability and access to personal data in a timely manner;

(6) establishing processes and protocols for testing the effectiveness of security measures; and

(7) implementing encryption measures of personal data during storage, transit, authentication process, or any measure that controls and limits access.

7. What restrictions, if any, are there on personal data being transferred to other jurisdictions? How would organizations generally address these restrictions?

Cross-border transfers are permissible, provided that: (1) the relevant data subjects are sufficiently informed of and consent to such transfer; and (2) third-party recipients enter into an agreement that includes certain "mandatory clauses" that ensure that the recipient will, among other things, comply with the requirements of the DPA and implement appropriate security measures. This also applies to the affiliated or related companies or entities belonging to the same group.

8. What restrictions, if any, are there on using or re-using personal data for data analytics/innovation or in adopting new business solutions such as artificial intelligence or data analytics? How would organizations generally address these restrictions?

Generally, the DPA does not restrict the use of personal information with respect to such types of technologies, provided that: (1) the relevant data subjects are sufficiently informed/notified of such use/purpose and that they consent thereto; and (2) reasonable and appropriate security measures are implemented.

9. What are the rights of an individual whose personal data is collected? Can they withdraw their consent, object to (and/or request deletion of) the retention of their personal data? If so, how?

The data subject has the right: (1) to be informed that their data is being processed; (2) to know the extent of the processing of such data (e.g., scope, purpose, to whom the data may be disclosed, period for storage); (3) to be informed of their rights to access and correct their data; (4) to have reasonable access to the data, to dispute inaccuracies or errors in their data; (5) to suspend the destruction of their data; and (6) to be indemnified for damages due to such inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of personal information. A data subject may withdraw consent to the retention of his/her personal information by a third party, although there is no specific process given in the DPA or in its IRR on withdrawing consent.

10. Are there any penalties, liabilities, or remedies if any of the personal information protection laws are violated?

There are mandatory fines (ranging from One Hundred Thousand Pesos to Five Million Pesos) and imprisonment terms (ranging from six (6) months to six (6) years). Additionally, a complaining data subject can seek civil damages (e.g., actual damages, moral damages, exemplary damages, etc.).

11. Is there mandatory data breach reporting in your jurisdiction? If so, could you summarize the thresholds that trigger reporting, what should be reported and to whom, and what timelines are required/expected?

Yes. Mandatory reporting to the NPC and notification to the affected data subjects arises if:

(1) sensitive personal information or any other information may, under the circumstances, be used to enable identity fraud;

(2) there is reasonable belief that such information may have been acquired by an unauthorized person; and

(3) the PIC or the NPC believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

These mandatory reporting and mandatory notification requirements must be made within 72 hours upon knowledge of, or when there is reasonable belief by the PIC or PIP that a personal data breach has occurred. This obligation is incumbent upon the PIC.

12. Are there any recent notable developments in your country or cases that you think are likely to affect data privacy/data protection in the future? Is there anything else you would like to highlight?

RNPC issued Circular No. 2022-01 dated 08 August 2022 (Circular, for brevity), which took effect on August 27, 2022, which fixes the amount of administrative fines that can be imposed by the NPC in the exercise of its quasi-judicial functions over complaints lodged with the NPC for infractions of DPA and its IRR and other issuances of the NPC. The Circular classified all violations into three categories with the corresponding range of imposable fines (computed as a percentage of the annual gross income of the immediately preceding year when the infraction occurred):

(1) Grave infractions - 0.5% to 3%

(2) Major infractions - 0.25% to 2%

(3) Other infractions - 0.25% to 2%

In no event shall the total imposable fine for a single act exceed Five Million Pesos (PhP5,000,000.00) (or around USD90,000.00).

Singapore

FIRM

Joyce A. Tan & Partners LLC
www.joylaw.com

CONTACT

Jeffrey Lim
Singapore, Singapore

Tel +65 6333 6383
jeffrey@joylaw.com

The firm is a dedicated commercial law firm that provides the full range of corporate and commercial legal services with particular strengths in intellectual property, technology, telecommunications, media, and privacy. We serve a broad range of industries on the international stage and have pioneered many forms of legal transactions on the cutting edge of significant trends and developments in business in Singapore.

In data protection and privacy, we advise on data protection laws and regulations and assist in developing policies and processes to comply with such laws and regulations globally. Our reputation is based as much on cross-border as it is on domestic work. Our clientele range from global MNCs (including "Big Tech" corporations) who seek us out, to nationally prominent corporations that work with us on key strategic projects, to established start-up technology clients. We provide focused solutions on matters of cybersecurity, data analytics, data mining, artificial intelligence, and content laws, as well as strategic and policy reviews.

Our service philosophy is to bring clarity and make the client experience a seamless, fuss-free encounter across multiple requirements.

1. What are the major personal data protection laws or regulations in your jurisdiction? Is there any cross-sector legislation, and does it prevail over sector-specific legislation or vice versa?

In Singapore, personal data is broadly regulated under the Personal Data Protection Act 2012 ("PDPA"), which governs the collection, use, disclosure, and processing of individuals' personal data by the private sector.

The PDPA is also supplemented by subsidiary legislation and various guidelines and guides issued by the Personal Data Protection Commission ("PDPC"). This includes practical tools such as guidelines on key concepts, the application of the PDPA and other topic and sector-specific guides (e.g., guides on the PDPA in areas like information and communication technology systems, blockchain design, biometric data in security systems, guarding against data breaches, and the education sector, etc.).

Sectoral regulators may also apply their own sector-specific laws that may have data protection or data privacy content, such as the Healthcare Services Act 2020, or specific rules and regulations under the Telecommunications Act 1999. In the event of any inconsistencies between the two, the standards and obligations imposed under other legislation would prevail over the PDPA.

2. Which regulatory authorities are responsible for the implementation and enforcement of personal information protection laws?

The PDPC is the agency responsible for the administration and enforcement of the PDPA.

3. How is "personal information"/"personal data" defined, and are there any categories of personal data that receive special or different protection (e.g., employees, minors, "sensitive" personal information, etc.)? If so, what are these categories, and can you summarize what special rules apply to these categories?

Personal data is defined as data, whether true or not, about an individual who can be identified:

(i) from that data; or

(ii) from other information to which the organization has or is likely to have access.

It therefore encompasses both direct and indirect identifiers.

While the PDPA does not specifically set out a class of "sensitive" personal data, the various rules and regulations under the PDPA for data breach

reporting mean that more stringent standards apply to data breaches involving data whose breach may result in significant harm.

Additionally, certain categories of personal data may be subject to differences in treatment in relation to the processing of personal data. For example, there are certain exceptions to the consent obligation where employees' personal data is concerned, and where the personal data of minors is concerned, there are specific guidelines that require additional safeguards to be put in place.

4. What are the key principles under the major personal data protection laws or regulations relating to personal data?

The PDPA does not articulate principles so much as set out key obligations which are as follows:

(1) **Consent:** Personal data can only be collected, used, or disclosed for purposes to which an individual has given their consent, unless the exceptions apply.

(2) **Notification:** Organizations must notify individuals of the intended purposes for the collection, use, or disclosure of their data.

(3) **Purpose Limitation:** Personal data can only be collected, used, or disclosed for purposes a reasonable person would consider appropriate under the given circumstances, and an organization must not require such consent as a condition to providing a product or service.

(4) **Accuracy:** An organization shall make a reasonable effort to ensure that personal data collected is accurate and complete if the personal data is likely to be used to make a decision affecting the individual or disclosed to another organization.

(5) **Protection:** An organization shall have in place reasonable security arrangements to protect the personal data in its possession to prevent unauthorized access, collection, use, disclosure, or similar risks.

(6) **Retention Limitation:** An organization shall cease retention or dispose of personal data in a proper manner when the data is no longer needed for any business or legal purpose.

(7) **Transfer Limitation:** Personal data may only be transferred to another country in accordance with the requirements prescribed under the PDPA and its regulations to ensure that the standard of protection is comparable to that under the PDPA.

(8) **Access and Correction:** Individuals will have the right to request access to their personal data, information on how the data was used or disclosed, and correction of any error or omission in their personal data.

(9) **Accountability:** An organization is responsible for personal data in its possession and control, and thus must undertake measures to ensure that it can meet its obligations under the PDPA and demonstrate that it can do so when required.

(10) **Data Breach Notification:** An organization must assess if a data breach is notifiable and notify the PDPC and affected individuals if so.

5. Are there any formal registration compliance requirements that apply to all businesses (e.g., the appointment of data protection officers, registration of databases, etc.)?

While there is no formal registration requirement, organizations must appoint one or more individuals as data protection officers ("DPO") to ensure the organization's compliance with the PDPA. The organization must make available the business contact information of the DPO by either registering the DPO with the Accounting and Corporate Regulatory Authority or providing the contact information in a readily accessible part of the organization's website.

6. What obligations are there for organizations to establish compliance programs (e.g., legal and operational policies, contracts, etc.) relating to the processing, use, and disclosure of personal data?

There are four main obligations for organizations in establishing compliance programs.

First, organizations must develop and implement data protection policies and practices to meet their obligations under the PDPA. Second, they must develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA. Third, organizations must inform and educate their staff about the organization's data protection policies and practices. Finally, organizations must also make information on their data protection policies, practices, and complaint process available upon request.

7. What restrictions, if any, are there on personal data being transferred to other jurisdictions? How would organizations generally address these restrictions?

Under the Personal Data Protection Regulations 2021, an organization may only transfer personal data overseas if appropriate steps have been taken to ensure that the overseas recipient is bound by legally enforceable obligations or specified certifications to provide the transferred data a standard of protection that is comparable to that under the PDPA.

This is a question of identifying a pathway to determining that there are legally enforceable obligations that would help to establish a means of

ensuring that the personal data receives the standard of protection required under the PDPA. Solutions accepted under the PDPA include adequate contractual requirements between transferor and transferee, reliance on binding corporate rules, other legally binding instruments, and so on.

8. What restrictions, if any, are there on using or re-using personal data for data analytics/innovation or in adopting new business solutions such as artificial intelligence or data analytics? How would organizations generally address these restrictions?

While it is the case that certain rules under the PDPA will place certain limitations around the use or re-use of personal data for analytics, innovation, and adoption of new solutions or artificial intelligence, Singapore has looked to address these by providing for exceptions to certain obligations under the PDPA and by issuing guidance to organizations on innovation and adoption of these technologies.

Examples of exceptions include the business improvement exception to the consent obligation which is particularly useful for cases for personalization of products or services or for identifying new solutions or opportunities. In order to apply the exception, certain processes and safeguards must be executed or in place. Another example of an exception includes the research exception to the consent for which other criteria and requirements may apply.

The PDPC has also issued guides and guidelines on topics such as the use of personal data in biometric solutions, blockchain, anonymization, and, as of the time of this publication, the PDPC is conducting a consultation on an upcoming guideline on the use of personal data for AI recommendation and decision systems.

9. What are the rights of an individual whose personal data is collected? Can they withdraw their consent, object to (and/or request deletion of) the retention of their personal data? If so, how?

An individual whose personal data has been collected may:

(a) withdraw their consent upon reasonable notice to the organization, and the organization (and its data intermediaries and agents) must cease collecting, using, or disclosing their personal data;

(b) request access to their personal data within an organization's possession or control and information about the ways that personal data had or may have been used or disclosed within a year before the request; and

(c) request correction to errors and omissions in personal data, upon which organizations must do so unless the organization is satisfied that there are reasonable grounds to deny such a request, with an additional duty to communicate the corrections to organizations who received the earlier erroneous data within a look-back period.

10. Are there any penalties, liabilities, or remedies if any of the personal information protection laws are violated?

Both individuals and organizations could face penalties for violation of the PDPA.

11. Is there mandatory data breach reporting in your jurisdiction? If so, could you summarize the thresholds that trigger reporting, what should be reported and to whom, and what timelines are required/expected?

Yes. Where there is reason to believe that a data breach affecting personal data has occurred, an organization must assess whether the breach is a notifiable one. A data breach would be notifiable if it results, or is likely to result, in significant harm to an affected individual or is, or is likely to be, of a significant scale. The threshold of significant harm is linked to the nature of the personal data compromised while significant scale refers to the number of individuals affected by the breach.

Notifications must be made within three (3) calendar days of the organization making the assessment of a notifiable breach. The notification should include facts of the data breach, details on how the data breach was handled, and the contact details of at least one authorized representative of the organization.

Notifications to affected individuals may also be required unless certain exceptions apply or if there are directions against giving such notifications. Where so, notifications must be in any manner that is reasonable in the circumstances. Aside from the facts of the breach, the notification should include the potential harm to the affected individual and details on the management by the organization of the data breach, as well as guidance on the steps affected individuals may take to protect themselves.

12. Are there any recent notable developments in your country or cases that you think are likely to affect data privacy/data protection in the future? Is there anything else you would like to highlight?

The Ministry of Communications and Information recently announced its plans to issue the Advisory Guidelines on the Use of Personal Data in AI Systems under the PDPA. With the growing prevalence of artificial intelligence, the guidelines would offer much-needed clarity on how developments in the AI space would be accounted for in terms of data protection.

Sri Lanka

FIRM

Neelakandan & Neelakandan
www.neelakandan.lk

CONTACT

Thishya Weragoda
Colombo, Sri Lanka

Tel +94 11 2371100
thishya.weragoda@neelakandan.lk

Neelakandan & Neelakandan (formerly Murugesu & Neelakandan) is one of the leading and oldest full-service law firms in Sri Lanka and has been in practice for more than 60 years.

The firm is entrusted with the protection in Sri Lanka of intellectual property of top world-renowned brands in both contentious and prosecution matters, and the firm handles a large volume of trade-mark, industrial design, and patent applications for a number of local, as well as foreign clients. The firm advises banking syndicates comprised of leading local and international banks in connection with financing arrangements for various infrastructure projects.

The dispute resolution practice of the firm covers all civil, commercial, and appellate litigation arising from a range of matters. The firm also has expertise in international arbitration and the enforcement of arbitral awards, admiralty, and shipping, and handles pre-litigation negotiations.

The firm advises domestic and international clients on commercial, corporate, and M&A matters. The firm also handles a range of real estate and construction transactional work and international shipping matters, and has a full-scope employment practice.

1. What are the major personal data protection laws or regulations in your jurisdiction? Is there any cross-sector legislation, and does it prevail over sector-specific legislation or vice versa?

The primary legal framework for safeguarding personal data in Sri Lanka is the Personal Data Protection Act, No. 9 of 2022 ("PDPA"). This law regulates the handling of personal data, enhances individuals' rights over their personal information, establishes a regulatory body for data protection, and other related matters.

Specialized legislation, such as the Computer Crime Act No. 24 of 2007, Electronic Transactions Act No. 19 of 2006, Right to Information Act No. 12 of 2016, Payment and Settlement Systems Act No. 28 of 2005, Banking Act No. 30 of 1988, Telecommunications Act No. 25 of 1991, and Intellectual Property Act No. 36 of 2003 also provide additional protection to personal data in specific instances and circumstances.

Although the Computer Crime Act does not explicitly define "data," Section 2 specifies its scope to encompass computers, computer systems, and "information affected" by such acts. Further, facilities or services, including any computer storage or data or information processing service, are also protected by the provisions of the Act.

Although privacy is not explicitly recognized as a fundamental right in Sri Lanka's constitution, Article 14A highlights privacy concerns within information access limitations.

In addition, the common law also provides a limited remedy as it recognizes a breach of privacy as a tort. Courts have also recognized the right to personal space.

2. Which regulatory authorities are responsible for the implementation and enforcement of personal information protection laws?

The Data Protection Authority (the "Authority") is the entity entrusted with enforcing the PDPA.

The Authority has the discretion to determine situations under which specific targeting of and monitoring of data subjects are permissible.

The Right to Information Act No. 12 of 2016 also provides a framework to review the release of information held by public authorities, where an Information Officer is empowered to decide whether to issue or release such information. That decision is open to appeal to a Designated Officer, whose decision, in turn, can be challenged before the Right to Information Commission.

The Payment and Settlement Systems Act No. 28 of 2005 also makes confidential all information collected by the Central Bank and any third party to whom such information is transmitted. Similar restrictions are placed in the Banking Act No. 30 of 1988.

3. How is "personal information"/"personal data" defined, and are there any categories of personal data that receive special or different protection (e.g., employees, minors, "sensitive" personal information, etc.)? If so, what are these categories, and can you summarize what special rules apply to these categories?

Section 56 of the PDPA defines "personal data" as pertaining to any information capable of directly or indirectly identifying an individual. This identification can be established through means such as a name, an identification number, financial details, location particulars, or an online identifier. Alternatively, personal data can be connected to specific factors related to the person's physical, physiological, genetic, psychological, economic, cultural, or social identity.

Distinct categories of personal data include information disclosing racial or ethnic origin, political viewpoints, religious or philosophical beliefs, genetic data processing, biometric data usage for uniquely identifying an individual, health-related information, and details concerning one's sexual life or sexual orientation, as well as data regarding criminal offenses, legal proceedings, and convictions, along with data related to minors.

The lawful processing of these special personal data categories is permissible, provided such processing is necessary for the pursuit, establishment, or defense of legal claims in a court of law, tribunal, or other judicial body.

The common law remedy of "actio injuriarum," based on Roman Dutch Law principles, provides a much wider scope of protection. This remedy has not been adequately explored in Sri Lanka despite there being no laws in place until the enactment of the PDPA in 2022.

4. What are the key principles under the major personal data protection laws or regulations relating to personal data?

The PDPA establishes safeguards for personal data held by various entities, including governmental bodies, banks, telecommunications companies, and medical facilities. Its main purpose is to strike a balance between individual rights and organizational interests, ensuring transparency and accountability in data processing procedures.

The legislation places responsibilities on individuals who handle personal information (Controllers and Processors as per the Act). Section 5 of the PDPA requires that organizations establish valid legal reasons for data processing, limiting it to these reasons, ensuring data accuracy and currency, setting retention limits, maintaining transparency, and protecting the confidentiality of personal information.

5. Are there any formal registration compliance requirements that apply to all businesses (e.g., the appointment of data protection officers, registration of databases, etc.)?

Section 20 of the PDPA requires every controller to designate or appoint a Data Protection Officer ("DPO") to ensure compliance with the PDPA where:

- Personal data is processed by a ministry, government body, department, or public corporation (excluding the judiciary in their judicial capacity); or
- Core processing activities involve:
  - regular and systematic monitoring of data subjects;
  - special categories of data;
  - a risk of harming data subjects' rights under the PDPA.

In cases where controllers are entities within a group, a single DPO can be designated. Public authorities acting as controllers or processors can appoint a single DPO for multiple authorities, considering their structures. DPO contact details must be published on websites. Regulatory authorities must be promptly informed about a DPO's appointment.

6. What obligations are there for organizations to establish compliance programs (e.g., legal and operational policies, contracts, etc.) relating to the processing, use, and disclosure of personal data?

Section 4 of the PDPA requires that every controller or business shall process personal data in compliance with the obligations imposed by the PDPA.

Obligations imposed on the controllers and processors include obligations to:

(a) process personal data in a lawful manner (s. 5 PDPA);

(b) define a purpose for personal data processing (s. 6 PDPA);

(c) confine personal data processing to the defined purpose (s. 7 PDPA;)

(d) ensure accuracy (s. 8 PDPA);

(e) limit the period of retention (s .9 PDPA);

(f) maintain Integrity and confidentiality (s. 10 PDPA);

(g) process personal data in a transparent manner (s. 11 PDPA); and

(h) implement internal controls and procedures for the purpose of complying with the obligations in this PDPA (s.12 PDPA).

Section 5 of the PDPA sets out instances under which personal data may be processed, including consent of the data subject, for the performance of contracts, emergencies, in the public interest, and legitimate interest.

7. What restrictions, if any, are there on personal data being transferred to other jurisdictions? How would organizations generally address these restrictions?

Public authorities must handle personal data as a controller or processor only within Sri Lanka, except where the relevant authority, in consultation with the involved controller/processor and Regulatory Authority, designates specific categories of personal data as eligible for processing in a third country under adequacy decisions made by the Minister.

Adequacy decisions by the Minister involve considering the laws and enforcement mechanisms in the third country in the context of relevant sections of the PDPA. Additional criteria may also be considered for cross-border data flow. Adequacy decisions must be periodically monitored and can be revised by the Minister in consultation with the Authority.

For organizations other than public authorities, controllers or processors can process personal data:

(a) in third countries specified by an adequacy decision; or

(b) in countries not covered by adequacy decisions, provided it ensures compliance with obligations in relevant sections of the PDPA.

To comply with (b) above, controllers or processors need to adopt instruments specified by the Authority. Such instruments must ensure that the recipient in the third country commits to enforceable safeguards protecting data subjects' rights and remedies under the PDPA.

In the absence of adequacy decisions or safeguards, organizations can still transfer data based on consent, contractual obligations, legal claims, public interest, emergencies, or other conditions mentioned in the PDPA.

8. What restrictions, if any, are there on using or re-using personal data for data analytics/innovation or in adopting new business solutions such as artificial intelligence or data analytics? How would organizations generally address these restrictions?

It is important to ensure compliance with the obligation to limit the period of retention under Section 9 of the PDPA.

Every controller may retain personal data only for such period as may be necessary or required for the purposes for which such personal data is processed. Under Section 10 of the PDPA, a controller may store personal data for longer periods if the personal data is archived for purposes in the public interest, scientific research, historical research, or statistical purposes.

9. What are the rights of an individual whose personal data is collected? Can they withdraw their consent, object to (and/or request deletion of) the retention of their personal data? If so, how?

The following rights of the data subjects are protected under the PDPA:

(a) Right to be informed:
Section 11 of the PDPA obliges controllers to provide the information referred to in Schedule V of the PDPA and information regarding any decision taken.

(b) Right of access to personal data:
Section 13 of the PDPA gives data subjects the right to access their personal data and be provided with a confirmation as to whether their personal data has been processed.

(c) Right of withdrawal of the consent:
Section 14 of the PDPA provides data subjects a right to withdraw their consent to processing at any time.

(d) Right to rectification or completion:
Section 15 of the PDPA entitles data subjects to request the controller to rectify or complete their personal data which is inaccurate or incomplete.

(e) Right to erasure:
Section 16 of the PDPA gives data subjects a right to have their personal data erased.

(f) Right not to be subject to automated decision-making:
Section 18 of the PDPA gives data subjects a right to request the controller to review decisions based solely on automated processing.

(g) Right to appeal:
Section 19 of the PDPA gives data subjects a right to appeal to the Authority against certain decisions of the controller.

Yes. Sections 14 and 16 of the PDPA grant data subjects the right to have their personal data erased upon a written request where:

(a) the processing of personal data is carried out in contravention of the obligations in Sections 5, 6, 7, 8, 9, 10, and 11 of the PDPA;

(b) the data subject withdraws the consent upon which the processing is based, in accordance with item (a) of Schedule I or item (a) of Schedule II of the PDPA;

(c) the requirement to erase personal data is required by any written law or on an order of a competent court to which the data subject or controller is subject.

10. Are there any penalties, liabilities, or remedies if any of the personal information protection laws are violated?

Yes. Under Section 38 of the PDPA, the PDPA provides for fines of up to Rs. 10 million for each instance of non-compliance. Repeat offenders may also be liable to pay an additional penalty consisting of twice the amount on the second and for each subsequent non-compliance.

11. Is there mandatory data breach reporting in your jurisdiction? If so, could you summarize the thresholds that trigger reporting, what should be reported and to whom, and what timelines are required/expected?

Yes. Under Section 23 of the PDPA, the data controller/processor must inform the Authority of a breach in such form, manner, and within such period of time as per the rules set out by the PDPA.

12. Are there any recent notable developments in your country or cases that you think are likely to affect data privacy/data protection in the future? Is there anything else you would like to highlight?

No.

Taiwan

FIRM

Formosan Brother Attorneys at Law
www.fblaw.com.tw/en/home

CONTACT

Li-Pu Lee
Taipei, Taiwan

Tel +866 2 2705 8086
lipolee@mail.fblaw.com.tw

Formosan Brothers Attorneys-at-Law was founded in 1997 and currently stands as one of Taiwan's preeminent full-service law firms in IP law, antitrust and competition, data protection, dispute resolution, real estate law, and corporate law. We have been providing our clients with high-quality legal services based on our belief in honesty, professionalism, responsibility, and teamwork, earning the trust and recognition of our clients. Many of our attorneys are licensed to practice both in Taiwan and foreign jurisdictions, contributing to our deep knowledge of international legal matters. What sets Formosan Brothers apart from our competitors, especially international law firms, is that our team of attorneys and consultants also receives legal training in Taiwan. As such, our team understands Taiwan's cultural and business nuances. Our international clients take comfort in knowing that we will combine both international knowledge and domestic understanding to craft the most suitable solutions to transnational matters.

1. What are the major personal data protection laws or regulations in your jurisdiction? Is there any cross-sector legislation, and does it prevail over sector-specific legislation or vice versa?

The Personal Data Protection Act ("PDPA") is the major personal data protection law in Taiwan, and this is the cross-sector data protection legislation that prevails over other local regulations and ordinances. However, the PDPA is the general guideline of the data protection law, and the legislature also authorizes the administrative branch to make different specific data protection rules such as the Directions for Personal Data Safety Maintenance by the Financial Supervisory Commission Designated Non-Government Entity.

2. Which regulatory authorities are responsible for the implementation and enforcement of personal information protection laws?

Taiwanese Legislature passed the Amendment to the Personal Data Protection Act of May 2023, designating the new Personal Data Protection Commission ("PDPC") as the exclusive Competent Authority for personal data protection in Taiwan.

3. How is "personal information"/"personal data" defined, and are there any categories of personal data that receive special or different protection (e.g., employees, minors, "sensitive" personal information, etc.)? If so, what are these categories, and can you summarize what special rules apply to these categories?

According to Article 2 of the PDPA, personal data refers to a natural person's name, date of birth, ID card number, passport number, features, fingerprints, marital status, family information, educational background, occupation, medical records, healthcare data, genetic data, data concerning a person's sex life, records of physical examination, criminal records, contact information, financial conditions, data concerning a person's social activities, and any other information that may be used to directly or indirectly identify a natural person. Article 6 specifies medical records, healthcare data, genetic data, data concerning a person's sex life, records of physical examination, and criminal records as sensitive personal information that the collecting and processing of is prohibited unless in certain exceptions.

4. What are the key principles under the major personal data protection laws or regulations relating to personal data?

Taiwan's PDPA does not specify the key principles such as the lawfulness, fairness, andtransparency in detail, but Article 5 generally states "the collection, processing and use of personal data shall be carried out in a way that respects the data subject's rights and interest, in an honest and good-faith manner, shall not exceed the necessary scope of specific purposes, and shall have legitimate and reasonable connections with the purposes of collection."

5. Are there any formal registration compliance requirements that apply to all businesses (e.g., the appointment of data protection officers, registration of databases, etc.)?

No, Taiwan's PDPA currently does not have formal registration compliance requirements that apply to all businesses.

6. What obligations are there for organizations to establish compliance programs (e.g., legal and operational policies, contracts, etc.) relating to the processing, use, and disclosure of personal data?

The duty to inform the data subject is required pursuant to Articles 8 and 9, and both government and non-government agencies shall expressly inform the data subject of the following information when collecting their personal data:

(1) the name of the government or non-government agency;

(2) the purpose of the collection;

(3) the categories of the personal data to be collected;

(4) the time period, territory, recipients, and methods for which the personal data is used;

(5) the data subject's rights under Article 3 and the methods for exercising such rights; and

(6) the data subject's rights and interests that will be affected if he/she elects not to provide his/her personal data.

The duty of informing data subject can be waived only under specific exceptions, such as where:

(1) the law grants a waiver;

(2) the collection of personal data is necessary for the government agency to perform its statutory duties or for the non-government agency to fulfil its statutory obligation;

(3) giving notice will prevent the government agency from performing its statutory duties;

(4) giving notice will harm public interests;

(5) the data subject already knows the content of the notification;

(6) the collection of personal data is for non-profit purposes and clearly has no adverse effect on the data subject;

(7) the personal data has been disclosed to the public by the data subject or has been made public lawfully;

(8) it is unable to inform the data subject or his/her statutory representative,

(9) it is necessary for statistics gathering or academic research in pursuit of public interests, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject; and

(10) the personal data is collected by mass communication enterprises for the purpose of news reporting for the benefit of public interests.

In addition, Article 5 requires that the collection, processing, and use of personal data shall be carried out in a way that respects the data subject's rights and interest, in an honest and good-faith manner, shall not exceed the necessary scope of specific purposes, and shall have legitimate and reasonable connections with the purposes of collection. These significant general data protection principles shall be carried out by means of correctly informing the data subject and may ultimately attain their consent (Article 8).

Moreover, Taiwan's PDPA requires government agencies in possession of personal data files shall assign dedicated personnel to implement security and maintenance measures to prevent the personal data from being stolen, altered, damaged, destroyed, or disclosed (Article 18).

As for the non-government agencies, there are the same requirements to assign dedicated personnel to implement security and maintenance measures (Article 27).

7. What restrictions, if any, are there on personal data being transferred to other jurisdictions? How would organizations generally address these restrictions?

Taiwan's PDPA only imposes restrictions on non-government agencies regarding the international data transfer under four circumstances (Article 21):

(1) where major national interests are involved;

(2) where an international treaty or agreement so stipulates;

(3) where the country receiving the personal data lacks proper regulations on the protection of personal data and the data subjects' rights and interests may consequently be harmed; and

(4) where the cross-border transfer of personal data to a third country (territory) is carried out to circumvent the PDPA;

For example, the Ministry of Culture of Taiwan pursuant to Article 21 prohibited the personal data retained by Apple Daily Taiwan from being transferred to its Hong Kong headquarters when Apple Daily suddenly announced its closure in mid-2021.

8. What restrictions, if any, are there on using or re-using personal data for data analytics/innovation or in adopting new business solutions such as artificial intelligence or data analytics? How would organizations generally address these restrictions?

Taiwan's PDPA does not have specific restrictions on using personal data for AI or innovative data analytics, but processors must follow the general rule in Article 5.

9. What are the rights of an individual whose personal data is collected? Can they withdraw their consent, object to (and/or request deletion of) the retention of their personal data? If so, how?

A data subject's rights under Taiwan's PDPA's Article 3 are:

(1) Right of Access and Inquiry (Article 10);

(2) Right of Data Portability (Article 14);

(3) Right to Rectification (Article 11);

(4) Right to Restrict Processing and Object (Article 11);

(5) Right of Erasure (Article 11 paragraph 3,4).

According to Article 20-2 and 19-2 of the Taiwan PDPA, a data collector or processor shall, on its own initiative or upon the request of the data subject, erase or cease processing or using the personal data when it becomes aware of such request, or upon being notified by the data subject. Thus, the data subject can certainly withdraw their consent or object to the processing or collection of their own data.

It should be noted that in terms of the Right of Erasure, the government or non-government agency shall, on its own initiative or upon the request of the data subject, erase or cease processing or using the personal data when the specific purpose of data collection no longer exists, or upon expiration of the relevant time period, or in the event where the collection, processing, or use of the personal data is in violation of the PDPA.

10. Are there any penalties, liabilities, or remedies if any of the personal information protection laws are violated?

The violation of the PDPA will result in civil liability (Articles 28-40), criminal liability (Articles 41-46), and administrative fines (Articles 47-50). The victims of the violation of the PDPA can also file a class action against the tortfeasor (Chapter IV of PDPA).

Our observation is that the two most common violations of the PDPA are:

(1) failure to give notice or exceeding the purpose limitation; and

(2) overlooking the implementation of reasonable safety measures to protect the data.

A violator of these two common violations will face civil liability (Articles 28,29), criminal prosecution (Articles 41), and administrative fines (Articles 47, 48).

For example, when a company illegally collects other people's medical records without giving proper notice to the data subjects, the company violates Article 6 and will be prosecuted under Article 41 with up to 5 years of imprisonment and an NT$1 million fine. Additionally, the government agency can impose an administrative fine between NT$50,000 and NT$500,000 based on Article 47. The company is also liable for the damages arising from any injury caused by their illegal conduct.

11. Is there mandatory data breach reporting in your jurisdiction? If so, could you summarize the thresholds that trigger reporting, what should be reported and to whom, and what timelines are required/expected?

Article 12 states that if any personal data is stolen, disclosed, altered, or otherwise infringed upon due to a violation of the PDPA by a government or non-government agency, the data subject shall be notified via appropriate means after the relevant facts have been clarified.

12. Are there any recent notable developments in your country or cases that you think are likely to affect data privacy/data protection in the future? Is there anything else you would like to highlight?

The public awareness of privacy rights and data protection in Taiwan has increased as fraud and scam crimes have recently become increasingly prevalent in the nation. The Taiwanese government has taken action to counter the invasion of privacy rights by both the public sector and private companies by amending the current PDPA. New measures include increasing administrative fines and establishing a new PDPC as the exclusive Competent Authority for personal data protection in Taiwan.

Thailand

FIRM

LawPlus Ltd.
www.lawplusltd.com

CONTACT

Kowit Somwaiya
Bangkok, Thailand

Tel +662 636 0662
kowit.somwaiya@lawplusltd.com

LawPlus Ltd. is a full-service law firm. Our top objective is to provide clients with high-quality and pragmatic legal advice and assistance in a timely manner while adding value to clients' business activities at a reasonable cost. We use our professional expertise and knowledge of the local and regional markets to assist our local and international clients to achieve their business objectives.

Our clients operate in a variety of industries, including automobile, construction, engineering, food and beverages, healthcare, hospitality, logistics, information and digital technology, telecommunications, retail and wholesale, e-commerce, and social media.

We advise and assist clients on domestic and cross-border commercial transactions, mergers and acquisitions, FDI, joint venture, governance and regulatory compliance, insolvency and debt restructuring, company registration and administration, employment and labor protection, banking and securities, intellectual property, trade competition, data privacy, telecommunications, media and technology, real property, digital assets, arbitration, litigation, inheritance, and probate.

LawPlus has been ranked as mid-to-top tier and recommended for several areas of practice by the Legal 500 and many other legal service ranking publications.

1. What are the major personal data protection laws or regulations in your jurisdiction? Is there any cross-sector legislation, and does it prevail over sector-specific legislation or vice versa?

The major personal data protection legislations of Thailand are the Personal Data Protection Act B.E. 2562 (A.D. 2018) ("PDPA") and the PDPA implementation and enforcement rules issued by the Personal Data Protection Committee ("PDPC") under the PDPA. The PDPA governs the processing (collection, use, and disclosure) of personal data by business operators and government offices as cross-sector legislation, except only in cases where sector-specific legislations apply but only to the extent that they are not contrary to the provisions of the PDPA.

2. Which regulatory authorities are responsible for the implementation and enforcement of personal information protection laws?

The PDPC is the regulatory authority in charge of implementing and enforcing the PDPA and its implementation rules and regulations. The PDPC issues implementation rules and regulations, establishes policies and directions for personal data protection, conducts investigations in response to complaints, and issues enforcement orders to data controllers and data processors who violate the PDPA.

The Office of the PDPC acts as the secretariat of the PDPC. The PDPC Office operates under the Ministry of Digital Economy and Society ("MDES").

Some sector-specific regulatory authorities, such as the Bank of Thailand in relation to commercial banks and other financial institutions, are also responsible for enforcing personal data protection under sector-specific legislations applicable to their respective sectors.

3. How is "personal information"/"personal data" defined, and are there any categories of personal data that receive special or different protection (e.g., employees, minors, "sensitive" personal information, etc.)? If so, what are these categories, and can you summarize what special rules apply to these categories?

The PDPA provides that "personal data means any information relating to a person, which enables the identification of such person, whether directly or indirectly, but not including the information of deceased persons."

The PDPA deals with two categories of personal data: (1) the general personal data and (2) the sensitive personal data ("SPD"). The SPD is the personal data "pertaining to racial, ethnic origin, political opinion, cult, religious or philosophical belief, sexual behavior, criminal records, health

data, disability, trade union information, genetic data, biometric data, or any other data which may affect the data subject in the same manner."

Collection of the SPD without explicit consent from the data subject is prohibited, except for a few exceptions, such as collection of the SPD for preventing or suppressing a danger to life, body, or health of the person where the data subject is incapable of giving consent for whatever reason.

Collection of personal data from a minor below the age of ten years requires consent from the holder of parental responsibility over the minor. Collection of personal data from a minor over ten years of age but is not sui juris by marriage or has no capacity as a sui juris person requires consent from the minor, and also consent from the holder of parental responsibility over the minor.

4. What are the key principles under the major personal data protection laws or regulations relating to personal data?

(1) The personal data can be collected only to the extent that the data is necessary for the purpose for which it is collected.

(2) The collected personal data can be retained for only for as long as necessary for the purposes of its use.

(3) The processing of the personal data can be carried out only in a manner where the integrity and confidentiality of the personal data is maintained and observed.

(4) The rights of data subjects to access, correct, object to processing, delete, and do other acts and things in relation to their personal data collected by data controllers or data processors must be fully recognized.

(5) A personal data breach can be subject to administrative fines, criminal liabilities, and civil liabilities.

5. Are there any formal registration compliance requirements that apply to all businesses (e.g., the appointment of data protection officers, registration of databases, etc.)?

There are no formal registration compliance requirements that apply to all businesses.

Any business which handles a large volume of SPD or processes a large amount of personal data must appoint a Data Protection Officer ("DPO") to ensure compliance with the PDPA and act as the contact person for data subjects and the PDPC.

All businesses must obtain express consent from data subjects before or upon collecting, using, or disclosing their personal data, except only where exceptions apply, and keep records of such consent.

Businesses who are data controllers or data processors must maintain records of their data processing activities and make them ready for inspection by or submission to the PDPC.

6. What obligations are there for organizations to establish compliance programs (e.g., legal and operational policies, contracts, etc.) relating to the processing, use, and disclosure of personal data?

The key compliance programs for organizations to have in place under the PDPA are as follows:

(1) Organizations must establish and maintain a data privacy policy that fully complies with the data processing requirements under the PDPA.

(2) A data processing agreement or a data transfer agreement between a data controller and a data processor must be fully compliant with the applicable requirements under the PDPA.

(3) When a business as a data controller carries out any high-risk data processing activity, it must carry out a Data Protection Impact Assessment ("DPIA") to identify data privacy risks and measures to mitigate such risks.

(4) Organizations must establish mechanisms to protect and facilitate the exercise of rights of data subjects, such as the right to access personal data, the right to withdraw consent at any time, the right to rectify, delete, restrict, or object to processing of personal data, the right to data portability, and the right to lodge a complaint with the PDPC Office.

7. What restrictions, if any, are there on personal data being transferred to other jurisdictions? How would organizations generally address these restrictions?

(1) The personal data cannot be transferred to a jurisdiction or an international organization that lacks adequate data protection, except only when explicit consent is given by the relevant data subjects after they have been informed of the lack of adequate data protection in the destination jurisdiction or destination international organization, or when the transfer of personal data is necessary under a contractual obligation of the transferor and the destination country or international organization.

(2) Organizations address these restrictions by (a) obtaining explicit consent from data subjects for cross-border data transfers, and (b) ensuring that contractual measures are in place to maintain data protection standards when data is transferred internationally, such as signing a data transfer agreement which contains a standard data protection clause.

(3) The PDPC encourages organizations to implement a set of their internal Binding Corporate Rules ("BCRs") to govern their intra-group data transfers to ensure that the companies in their group adopt a high standard of data protection to govern their intra-group personal data transfers.

8. What restrictions, if any, are there on using or re-using personal data for data analytics/innovation or in adopting new business solutions such as artificial intelligence or data analytics? How would organizations generally address these restrictions?

The PDPA does not differentiate between the automated means and the non-automated means of personal data processing (using or re-using).

If organizations plan to use or re-use personal data for data analytics, artificial intelligence, or innovation, they should disclose (in their privacy notice or request for consent) such processing to the relevant data subjects upon or prior to the collection of their personal data.

9. What are the rights of an individual whose personal data is collected? Can they withdraw their consent, object to (and/or request deletion of) the retention of their personal data? If so, how?

Please refer to 6(4) above. The privacy notice from the data controller to data subjects must list all the rights of data subjects and include provisions on how and when data subjects can exercise their rights.

Data subjects can exercise their right to withdraw their consent for processing their personal data any time by way of giving a notice to the data controller or the data processor.

10. Are there any penalties, liabilities, or remedies if any of the personal information protection laws are violated?

Data controllers and data processors who violate the PDPA legislations can be subject to: (1) administrative fines, (2) criminal liabilities, and (3) civil liabilities.

The maximum administrative fine is THB5 million.

The criminal penalties include the maximum imprisonment of one year and/or the maximum fine of THB1 million per count of violation.

The civil liabilities are the compensation for actual damages and punitive damages payable to the injured data subject as the Court may order.

Penalties imposed by the PDPC or the Court can vary depending on the nature, severity, and duration of the violation, the number of the affected data subjects, and the mitigation measures implemented by the violator upon the occurrence of the violation.

11. Is there mandatory data breach reporting in your jurisdiction? If so, could you summarize the thresholds that trigger reporting, what should be reported and to whom, and what timelines are required/expected?

If a data breach that could pose risks to the rights and freedoms of data subjects occurs, the data controller must report the breach to the PDPC Office within 72 hours after having become aware of the breach. The report must include the nature of the breach, the details of the contact person or the DPO of the data controller, the possible consequences, and the measures taken or to be taken to mitigate the potential adverse effects.

If the data breach poses a high risk to the rights and freedoms of the data subjects, the data controller must also inform the affected data subjects of the breach without undue delay.

12. Are there any recent notable developments in your country or cases that you think are likely to affect data privacy/data protection in the future? Is there anything else you would like to highlight?

The PDPA came into full force and effect on and from 1 June 2022.

As of June 2023, the PDPC has issued 14 implementation rules, regulations, and guidelines on personal data processing (collection, use, and disclosure), recording of processing activities, personal data breach reports, etc.

The MDES, the PDPC and the PDPC Office, and the private sector have been implementing a large number of programs to promote the digital economy, cybersecurity, and personal data protection amongst the private and public sectors.

Personal data protection legislations and practices are new and still evolving. Organizations operating in Thailand or related to the processing of personal data collected in or transferred from Thailand should closely monitor the development, practice, and enforcement of the data privacy legislations of Thailand.

Vietnam

FIRM

Russin & Vecchi
www.russinvecchi.com.vn

CONTACT

Viet T Le
Ho Chi Minh City, Vietnam

Tel +84 28 3824 3026
ltviet@russinvecchi.com.vn

Russin & Vecchi was founded in Asia over 50 years ago to serve emerging economies. It has several affiliated but independent offices in Russia, Taiwan, Thailand, the Dominican Republic, New York, and elsewhere.

Russin & Vecchi had an office in Vietnam from 1966 to 1975, which it reopened in 1993, with Heineken as its first client. Our history in Vietnam is simply unique. We have strong ties and broad experience in the country and have been at the forefront of Vietnam's development since our founding.

Our team is comprised of 4 partners and 20 lawyers with offices in both Ho Chi Minh City and Hanoi and united by many years in a strong collegial culture. As the oldest law firm in Vietnam, we have been part of many ground-breaking transactions and have helped create solutions previously untried.

1. What are the major personal data protection laws or regulations in your jurisdiction? Is there any cross-sector legislation, and does it prevail over sector-specific legislation or vice versa?

In Vietnam, the right to privacy and personal secrets is a constitutional right. Prior to July 1, 2023, data protection requirements were provided in numerous legislative documents, including the Civil Code 2015 (November 24, 2015) (the "Civil Code") and the Law on Cyber Information Security No. 86/2015/QH13 (November 19, 2015) ("LCIS"). Provisions on data protections are also provided in sectoral laws such as the Law on Electronic Transactions No. 51/2005/QH11 (November 29, 2005) and the Law on Telecommunications No. 41/2009/QH12 (November 23, 2009), and various other sectoral laws. On April 17, 2023, the Government issued Decree 13/2023/ND-CP on the protection of personal data ("Decree 13"), which became effective on July 1, 2023. Decree 13 is the Government's first step toward consolidating the regulations on personal data.

2. Which regulatory authorities are responsible for the implementation and enforcement of personal information protection laws?

The Ministry of Public Security ("MPS") is the supervisory authority for data protection. The Department of Cybersecurity and Prevention of Cyber-Crimes under the MPS ("A05 Department") is the specialized task force established to implement and enforce data protection regulations, including Decree 13.

3. How is "personal information"/"personal data" defined, and are there any categories of personal data that receive special or different protection (e.g., employees, minors, "sensitive" personal information, etc.)? If so, what are these categories, and can you summarize what special rules apply to these categories?

"Personal data" is defined to be any information in the form of symbols, letters, numbers, graphics, audio, or any other form in a digital environment related to the identification of a particular natural person or, when combined with other data, which can be used to identify a particular natural person. Personal data is divided into basic personal data and sensitive personal data. Protection of personal data in general requires the implementation of appropriate technical and management measures and the preparation and publishing of data protection policies. On the other hand, protection of "sensitive personal data" further requires the establishment of a data protection department and the appointment of a person in charge of protecting personal data (i.e., a data protection officer).

4. What are the key principles under the major personal data protection laws or regulations relating to personal data?

The key principles for data protection under Decree 13 can be summarized as follows:

- the data subject must be informed of the specifics of the processing activities, unless otherwise required by law;
- the data subjects must consent to the processing activities. Consent must be voluntary, specific, and verifiable. Consent may be withdrawn or conditional. Data can be processed without consent under certain circumstances.
- personal data must be processed according to the purposes for which the data subjects have been informed and have consented;
- personal data must only be collected to the extent necessary for the scope and purposes of data processing. Sales and purchase of personal data in any manner is prohibited unless otherwise provided by laws;
- personal data provided must be accurate, true, and complete, and be updated and supplemented appropriately.
- personal data must be protected by security measures; and
- personal data may only be stored for as long as necessary to serve the processing purposes.

5. Are there any formal registration compliance requirements that apply to all businesses (e.g., the appointment of data protection officers, registration of databases, etc.)?

Any party, who qualifies as either a data controller or a data processor under Decree 13 is required to prepare, maintain, and submit to the A05 Department a personal data processing impact assessment ("PDPIA"). The PDPIA does not need to be approved, but the MPS A05 Department may request the transferor to provide additional supporting documents. The contents of the PDPIAs for data controllers and data processors differ. PDPIAs must be submitted to the AO5 Department within 60 days of commencement of the personal data processing activities.

PDPIAs must include the following content:

- information and contact details of the data controller or data processor;
- name and contact details of the data protection department and officers of the data controller;
- purpose of the personal data processing activities;
- description of the processing activities (only applicable to data processors) and the types of personal data to be processed;

- receiver of personal data, including offshore receiver;
- offshore transfer of personal data (if any);
- duration of the data processing activities, potential reasons for deletion or removal of personal data (if any);
- description of implemented protection measures; and
- assessment of the impacts of personal data processing activities;
- potential unwanted consequences and mitigation measures.

6. What obligations are there for organizations to establish compliance programs (e.g., legal and operational policies, contracts, etc.) relating to the processing, use, and disclosure of personal data?

Decree 13 provides a general requirement for any individual or entity involved in the processing of personal data to develop and adopt policies on protection of personal data in compliance with regulations on data protection. Decree 13 does not require any specific policy or program. On the other hand, Decree 13 requires the PDPIA to include a description of implemented protection measures, which include all established and adopted policies.

7. What restrictions, if any, are there on personal data being transferred to other jurisdictions? How would organizations generally address these restrictions?

Under Decree 13, the transfer of personal data is considered a processing activity. As such, general requirements for the processing of personal data apply. Additionally, an entity or individual, that transfers personal data outside of Vietnam or uses offshore facilities to process the personal data of Vietnamese nationals must prepare and maintain a Data Transfer Impact Assessment ("DTIA"). DTIAs must be submitted to the AO5 Department within 60 days after the transferor begins to process personal data. After the transfer is complete, the transferor must notify the A05 Department. The DTIA does not need to be approved, but the A05 Department may request the transferor to provide additional supporting documents.

The DTIA must include the following content:

- information and contact details of the transferor and receiver;
- full name and contact details of the entity or individual transferor directly involved with the transfer and receipt of the personal data of Vietnamese Nationals;
- description and explanation of the purposes of the processing activities to be performed after such transfer;
- description of the types of data to be transferred;

- description of the compliance with the requirements of Decree 13 and a description of applied security measures;
- assessment of the impact of the data processing activities, potential consequences, mitigation, and/or prevention measures;
- consent of the data subjects, including a mechanism for the data subjects to respond to or file a claim upon the occurrence of any incident; and
- a binding document between the transferor and the receiver, outlining the rights and obligations and responsibilities of each party.

8. What restrictions, if any, are there on using or re-using personal data for data analytics/innovation or in adopting new business solutions such as artificial intelligence or data analytics? How would organizations generally address these restrictions?

There are no special restrictions on using or re-using personal data for data analytics/innovation or in adopting new business solutions such as artificial intelligence. The general requirements for processing of personal data apply.

9. What are the rights of an individual whose personal data is collected? Can they withdraw their consent, object to (and/or request deletion of) the retention of their personal data? If so, how?

An individual whose personal data is collected and processed is a data subject for the purposes of Decree 13.

A data subject has the following rights:

- the right to be informed of the method, scope, location, and purposes of the collection, processing, and use of their personal data;
- the right to access, or to request access to view or edit their personal data;
- the right to give or to withdraw consent to the processing of their personal data;
- the right to delete their personal data or to request that their personal data be deleted;
- the right to object to, or to restrict, data processing activities;
- the right to request that the data controller provide a copy of their personal data; and
- the right to claim for damages, to initiate legal proceedings, and to implement measures for self-protection.

10. Are there any penalties, liabilities, or remedies if any of the personal information protection laws are violated?

Non-compliance with data protection laws can result in both administrative penalties and criminal penalties. Under Decree 15/2020/ND-CP (February 3, 2022), as amended by Decree 14/2022/ND-CP (January 27, 2022), administrative penalties may include fines up to VND 70 million (approximately US$2,961) for each violation, subject to the decision of the enforcing authority. Criminal penalties may be imposed for violations of rules governing confidentiality and safety concerning an individual's email, mail, telephone, or other forms of communication. The government is working on additional sanctions for violations of personal data protection rules, which may increase the administrative penalty up to 5% of the violating entity's total revenues in Vietnam.

11. Is there mandatory data breach reporting in your jurisdiction? If so, could you summarize the thresholds that trigger reporting, what should be reported and to whom, and what timelines are required/expected?

Data processors are required to notify data controllers as soon as possible upon becoming aware of a data breach. Data processors and controllers are required to notify the A05 Department within 72 hours of the occurrence of a data breach. If the notification is not made within 72 hours, an explanation is required.

Notifications must include the following content:

- description of the nature and scope of the data breach, including but not limited to the time of the occurrence, the location, and the breached data and information of the parties involved;
- contact information of the person in charge of personal data protection;
- description of the consequences or damages of the data breach;
- description of the measures that have been applied to handle or mitigate the consequences or damages of the data breach.

12. Are there any recent notable developments in your country or cases that you think are likely to affect data privacy/data protection in the future? Is there anything else you would like to highlight?

The MPS will establish a National Portal on Data Protection (the "Portal"), which will be the central hub for data processors and data controllers to submit reports, impact assessments, and notifications. The Portal will also provide further guidance on current and future regulations on data protection. The Portal is expected to be available in July 2023.

On August 15, 2022, the government issued Decree 53/2022/ND-CP (August 15, 2022) ("Decree 53"). Among other things, Decree 53 provides important guidance and clarification on "data localization" and "mandatory physical establishment" requirements introduced by the Law on Cybersecurity.

Decree 53 regulates the following "regulated data":

- personal data of Vietnam-based users;
- data created by Vietnam-based users, including account name, time of usage, credit card information, email address, IP address, most recent log-out, and registered phone number; and
- data relating to the relationship of Vietnam-based users to users' friends or other people with whom the users interact.

Under Decree 53, a Vietnamese company must store regulated data in Vietnam. A foreign enterprise doing business in Vietnam would be required to store regulated data in Vietnam and establish a branch or a representative office, should it fall under certain circumstances, including, among others, having its services used to violate the Law on Cybersecurity.

MERITAS®

www.meritas.org